Université des Sciences et Technologies de Lille
U.F.R. de Mathématiques Pures et Appliquées

M209 : Approximation et fractions continues

Notes de cours par Clément Boulonne

L2 Mathématiques **2007 - 2008**

Table des matières

Chapitre 1

Développement en fractions continues

Introduction

Proposition 1.0.1. *Tout nombre réel est limite d'une suite de nombres rationnels. ($\mathbb{Q}$ est dense dans $\mathbb{R}$).*

Démonstration. Soit $\alpha \in \mathbb{R}$, $\forall n \in \mathbb{N}$:

$$10^n\alpha - 1 \leq E(10^n\alpha) \leq \alpha 10^n$$

$$\alpha - \frac{1}{10}^n \leq \frac{E(10^n\alpha)}{10^n} \leq \alpha$$

où E désigne la partie entière. Si on prend $n \to \infty$ alors :

$$\lim_{n\to+\infty} \alpha - \frac{1}{10^n} = \alpha$$

$$\lim_{n\to+\infty} \alpha = \alpha$$

Par le théorème des gendarmes, on peut en déduit :

$$\lim \frac{E(10^n\alpha)}{10^n} = \alpha$$

□

Le problème que l'on se pose est le suivant. Soit $\alpha \in \mathbb{R}$. Soit N un entier. Trouver la meilleure approximation de α par un nombre rationnel $\frac{a}{b}$ tel que $b \leq N$. Autrement dit, il faut trouver le nombre rationnel $\frac{a}{b}$ le plus "proche" de α avec $b \leq N$.

1.0.1 Exemple de fractions continues

Algorithme d'Euclide pour la division euclidienne

Exemple 1.0.1. On veut trouver PGCD$(30, 13)$.

$$30 = 13 \times 2 + 4$$

$$13 = 4 \times 3 + 1$$

Sous forme de fractions :

$$\frac{30}{13} = 2 + \frac{4}{13}$$

$$\frac{13}{4} = 3 + \frac{1}{4}$$

Si on regroupe le tout :

$$\frac{30}{13} = 2 + \frac{1}{3 + \frac{1}{4}}$$

Notation. On note cette fraction : $\frac{30}{13} = [2, 3, 4]$

Exemple 1.0.2. Soit $\alpha = \frac{1+\sqrt{5}}{2}$ le nombre d'or. On a : $\alpha^2 = \alpha + 1 \Rightarrow \alpha = 1 + \frac{1}{\alpha}$.

$$\alpha = 1 + \frac{1}{1 + \frac{1}{\alpha}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\alpha}}} = \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}}$$

C'est une fraction continue infinie.

1.1 Fractions continues

Définition 1.1.1. Soient $(a_i)_{i \in \mathbb{N}}$ une suite de nombres réels.

– L'expression :

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \; a_{n-1} + \frac{1}{a_n}}}}$$

est appelée une fraction continue finie. On la note $[a_0, a_1, a_2, ..., a_{n-1}, a_n]$

– L'expression :

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \; a_{k-1} + \frac{1}{a_k} \; \ddots}}}$$

qu'on note $[a_0, a_1, ..., a_k, ...]$ est dite une fraction continue infinie.

Définition 1.1.2. La fraction continue est dite simple si tous les coefficients a_i sont des entiers (dans $\mathbb{Z}$).

Définition 1.1.3. La fraction infinie continue est dite convergente si la suite des rationnels $(A_n)_{n \to \mathbb{N}}$ définie pr :

$$A_n = [a_0, ..., a_n]$$

converge dans $\mathbb{R}$.

Définition 1.1.4. La fraction continue finie $A_n = [a_0, ..., a_n]$ est appelée la n-ième réduite de la fraction continue.

Remarque. (i) On a :

$$[a_0, ..., a_n] = a_0 + \frac{1}{[a_1, ..., a_n]}$$

(ii) On a :

$$\underbrace{[a_0, ..., a_n]}_{n+1 \text{ coef}} = \underbrace{\left[a_0, ..., a_{n-1} + \frac{1}{a_n}\right]}_{n \text{ coef}}$$

Proposition 1.1.1. *Soient $a_0, a_1, ..., a_k$ une suite finie ou infinie d'entiers vérifiant :*

$$a_k \geq 1 \text{ pour tout } k \geq 1$$

Soient $(p_n)_{n\in\mathbb{N}}$ et $(q_n)_{n\in\mathbb{N}}$ les suites d'entiers définies par :

$$[a_0, ..., a_n] = \frac{p_n}{q_n} \text{ avec } PGCD(p_n, q_n) = 1,\ q_n > 0$$

Alors pour tout $\alpha \in \mathbb{R}^*$ et pour tout $n \geq 1$:

$$[a_0, ..., a_n, \alpha] = \frac{\alpha p_n + p_{n+1}}{\alpha q_n + q_{n+1}}$$

Notons $(\mathcal{P}_n)$: $\forall n \in \mathbb{R}^*$, $[a_0, ..., a_n, \alpha] = \dfrac{\alpha p_n + p_{n+1}}{\alpha q_n + q_{n+1}}$ et $|p_n q_{n+1} - q_n p_{n+1}| = 1$

Démonstration. Par reccurence sur n. Remarquons d'abord que :

$$[a_0] = a_0 = \frac{p_0}{q_0}$$

$$\text{PGCD}(p_0, q_0) = 1 \Rightarrow p_0 = a_0,\ q_0 = 1 \text{ par le lemme de Gauss.}$$

On calcule :

$$[a_0, a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}$$

Or $\text{PGCD}(a_0a_1+1, a_1)|a_0a_1$ et $\text{PGCD}(a_0, a_1+1)|a_0a_1+1 \Rightarrow \text{PGCD}(a_0a_1+1)|a_0a_1 - a_0a_1+1 \Rightarrow$ $\text{PGCD}(a_0a_1 + 1, a_1) = 1$.

Alors $p_1 = a_0a_1 + 1$ et $q_1 = a_1$. Vérifions que $(\mathcal{P}_1)$ est vraie :

$$[a_0, a_1, \alpha] = a_0 + \frac{1}{a_1 + \frac{1}{\alpha}} = a_0 + \frac{\alpha}{a_1\alpha + 1}$$

$$= \frac{(a_0a_1)\alpha + a_0}{a_1\alpha + 1} = \frac{p_1\alpha + p_0}{q_1\alpha + q_0}$$

Mais il faut vérifier que :

$$|p_1q_0 - q_1p_0| = 1$$

Or :

$$p_1q_0 - q_1p_0 = a_0a_1 + 1 - a_1a_0 = 1$$

On suppose que $(\mathcal{P}_n)$ est vérifée. Remarquons d'abord que $(\mathcal{P}_n)$ avec $\alpha = a_{n+1}$

$$\Rightarrow [a_0, ..., a_n, a_{n+1}] = \frac{p_n a_{n+1} + p_{n+1}}{q_n a_{n+1} + q_{n+1}}$$

Or :

$$q_n(a_{n+1}p_n + p_{n+1}) - p_n(q_n a_{n+1} + q_{n+1})$$
$$= q_n p_{n+1} - p_n q_{n-1} = \pm 1 \text{ d'après}(\mathcal{P}_n)$$

Donc : PGCD$(p_n a_{n+1} + p_{n+1}, q_n a_{n+1} + q_{n+1}) = 1$. D'où :

$$p_{n+1} = p_n a_{n+1} + p_{n-1},\ q_{n+1} = q_n a_{n+1} + q_{n-1}$$

Montrons que $(\mathcal{P}_{n+1})$ est vérifiée :

$$[a_0, ..., a_n, a_{n+1}, \alpha] = \left[a_0, ..., a_n, a_{n+1} + \frac{1}{\alpha}\right]$$

On pose : $\beta = a_{n+1} + \frac{1}{\alpha} \in \mathbb{R}^*$. D'après l'hypothèse de réccurence, on a :

$$[a_0, ..., a_{n+1}, \alpha] = [a_0, ..., a_n, \beta] = \frac{\beta p_n + p_{n+1}}{\beta q_n + q_{n+1}}$$

$$= \frac{(a_{n+1} + \frac{1}{\alpha})p_n + p_{n+1}}{(a_{n+1} + \frac{1}{\alpha})q_n + q_{n+1}} = \frac{\alpha a_{n+1} p_n + p_n + \alpha p_{n-1}}{\alpha a_{n+1} q_n + q_n + \alpha q_{n-1}}$$

$$= \frac{\alpha(a_{n+1} p_n + p_{n-1}) + p_n}{\alpha(a_{n+1} q_n + q_{n+1}) + q_n} = \frac{\alpha p_{n+1} + p_n}{\alpha q_{n+1} + q_n}$$

Il faut maintenant montrer que :

$$|p_{n+1} q_n - q_{n+1} p_n| = 1$$

$$p_{n+1} q_n - q_{n+1} p_n = (a_{n+1} p_n + p_{n+1}) q_n - (a_{n+1} q_n + q_{n+1}) p_n$$

$$= p_{n-1} q_n - q_{n-1} p_n = \pm 1$$

Donc : $(\mathcal{P}_{n+1})$ est vérifiée. □

Corollaire. *Soient $a_0, ..., a_k$ une suite d'entiers vérifiant $a_k \geq 1$ pour $k \geq 1$. Soient $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$ la suite des réduites associées à la suite (a_i), c'est-à-dire $[a_0, ..., a_n] = \frac{p_n}{q_n}$ avec PGCD$(p_n, q_n) = 1$ et $q_n \geq 1$ pour tout $n \in \mathbb{N}$. Alors les suites $(p_n), (q_n)$ sont définies par reccurence :*

$$p_0 = a_0,\ p_1 = a_0 a_1 + 1\,;\ \forall n \geq 2,\ p_n = a_n p_{n-1} + p_{n+2}$$

$$q_0 = 1,\ q_1 = a_1\,;\ \forall n \geq 2,\ q_n = a_n q_{n-1} + q_{n-2}$$

De plus, on a :

1) pour tout $n \geq 1$, $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$ ou :

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^n}{q_n q_{n-1}}$$

2) pour tout $n \geq 2$, $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$

3) pour tout $n \in \mathbb{N}$, on a : $q_{n+1} > q_n$ donc $q_n \geq n$.

Démonstration. 1) Les formules de reccurence découlent de la **Proposition 1.1.1.**

2) On a :

$$p_n q_{n-2} - p_{n-2} q_n = (a_n p_{n-1} + p_{n-2}) q_{n-2} + (a_n q_{n-1} + q_{n-2}) p_{n-2}$$

$$= a_n(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = a_n \times (-1)^n \text{ d'après 1)}$$

3) On a :

$$q_{n+1} = \underbrace{a_{n+1}q_n}_{\geq q_n} + \underbrace{q_{n-1}}_{\geq q_n} \Rightarrow q_{n+1} \geq q_n$$

Et comme $q_1 > 1$ donc $q_n > n$.

□

Proposition 1.1.2. *Soit $(a_i)_{i\in\mathbb{N}}$ des entiers vérifiant $a_i \geq 1$ pour tout $i \geq 1$. Soit $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$ la suite des véhicules associée à la suite (a_i). Alors on a :*

(i) les suites $\left(\frac{p_{2n}}{q_{2n}}\right)_{n\in\mathbb{N}}$ et $\left(\frac{p_{2n+1}}{q_{2n+1}}\right)_{n\in\mathbb{N}}$ sont adjaçante et on a :

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < ... < \frac{p_{2k}}{q_{2k}} < ... < \frac{p_{2k+1}}{q_{2k+1}} < ... < \frac{p_1}{q_1}$$

(ii) Toute fraction continue simple infinie est convergente.

Démonstration. Posons $b_n = \frac{p_n}{q_n}$. D'après le **Corollaire** précédent, on a :

$$b_n - b_{n-2} = \frac{(-1)^n a_n}{q_n q_{n-2}}$$

car $p_n q_{n-2} - q_n p_{n-2} = (-1)^n a_n$ $(n \geq 2)$.

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_n q_{n-2}}$$

Le signe de $b_n - b_{n-2}$ est de signe $(-1)^n$. Donc : la suite (b_{2n}) est croissante et la suite (b_{2n+1}) est décroissante.

Or : d'après le **Corollaire**, on a : $\forall n \geq 1$:

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-2}}$$

Donc : $b_n - b_{n-1} = \frac{(-1)^n}{q_n q_{n-1}}$. On en conclut que : $b_{2n+1} - b_{2n} > 0$. On a :

$$b_{2n+1} - b_{2n} = \frac{1}{q_{2n+1}q_{2n}} \geq \frac{1}{(2n+1)2n}$$

Quand $n \to \infty$:

$$\frac{1}{(2n+1)2n} \to 0$$

Donc les suites (b_{2n}) est (b_{2n+1}) sont adjaçantes. Donc elles convergent vers une même limite ℓ. Donc la suite $(b_n)_{n\in\mathbb{N}}$ converge vers ℓ. □

Exemple 1.1.1. $\alpha = \frac{1+\sqrt{5}}{2}$, (a_i) définie pour $a_i = 1$ pour tout i :

$$\frac{p_n}{q_n} = \underbrace{[1, 1, ..., 1]}_{n+1 \text{ fois}}$$

$\left(\frac{p_n}{q_n}\right)$ converge.

Proposition 1.1.3. *Soient $(a_i)_{i\in\mathbb{N}}$ et $(b_j)_{j\in\mathbb{N}}$ deux suites d'entiers telles que $a_i \geq 1$ et $b_j \geq 1$ pour tout $i \geq 1$ et $j \geq 1$. Alors,*

(i) si $[a_0, ..., a_n] = [b_0, ..., b_m]$ *et* $a_n > 1$ *et* $b_n > 1$ *alors* $n = m$ *et* $a_i = b_i$ *pour tout* $0 \leq 1 \leq n$.

(ii) si $[a_0, ..., a_n, ...] = [b_0, ..., b_n, ...]$ *alors* $a_i = b_i$ *pour tout* $i \in \mathbb{N}$.

Démonstration. (i) Remarquons que tout $1 \leq i \leq n$:

$$[a_i, ..., a_n] > a_i \geq 1 \qquad [b_i, ..., b_n] > b_i \geq 1$$

$$[a_0, ..., a_n] = a_0 + \frac{1}{[a_1, ..., a_n]}$$

$\Rightarrow E([a_0, ..., a_n]) = a_0$ et $E([b_0, ..., b_n]) = b_0$. Si $[a_0, ..., a_n] = [b_0, ..., b_n]$ et $a_n > 1$ et $b_n > 1$ on a : $a_0 = b_0$.

Donc : $[a_1, ..., a_n] = [b_1, ..., b_n]$, d'où $E([a_1, ..., a_n]) = E([b_1, ..., b_n]) \Rightarrow a_1 = b_1$ car $[a_2, ..., a_n] > 1$ et $[b_2, ..., b_n] > 1$. Ainsi de suite...

(ii) Supposons que $[a_0, ..., a_n, ...] = [b_0, ..., b_n, ...]$. On peut poser :

$$\lim_{n \to +\infty} [a_0, ..., a_n] = [a_0, ..., a_n, ...]$$

$$\lim_{n \to +\infty} [a_0, ..., b_n] = [a_0, ..., b_n, ...]$$

$E([a_0, ..., a_n])$?, on a :

$$[a_0, .., a_n, ...] = a_0 + \frac{1}{\beta} \text{ avec } \beta = [a_i, ..., a_n, ...]$$

Donc : $\beta > 1$ car $a_i > 1$. Donc : $E([a_0, ..., a_n, ...]) = a_0$, de même $E([b_0, ..., b_n, ...]) = b_0$. Donc : $a_0 = b_0$.

Supposons que pour tout $0 \leq i \leq n$, on a $b_i = a_i$. On montre alors que $a_{n+1} = b_{n+1}$. Posons :

$$\alpha_{n+1} = [a_{n+1}, ...] \qquad \beta_{n+1} = [b_{n+1}, ..]$$

On a : $[a_0, ..., a_n, \alpha_{n+1}] = [a_0, .., a_n, \beta_{n+1}]$ par hypothèse de reccurence.

D'après **Proposition 1.1.1.**, on a :

$$[a_0, ..., a_n, \alpha_{n+1}] = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}$$

où $\frac{p_k}{q_k}$ est la $k$ième réduite associée à la suite $a_0, ..., a_k$, $0 \leq k \leq n$.

$$[a_0, ..., a_n, \beta_{n+1}] = \frac{\beta_{n+1} p_n + p_{n-1}}{\beta_{n+1} p_n + p_{n+1}}$$

Donc :

$$\begin{aligned} & \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}} = \frac{\beta_{n+1} p_n + p_{n-1}}{\beta_{n+1} q_n + q_{n-1}} \\ \Rightarrow \quad & (p_n q_{n-1} - q_n p_{n-1})(\alpha_{n+1} - \beta_{n+1}) = 0 \\ \Rightarrow \quad & |\alpha_{n+1} - \beta_{n+1}| = 0 \\ \Rightarrow \quad & \alpha_{n+1} = \beta_{n+1} \\ \Rightarrow \quad & E(\alpha_{n+1}) = E(\beta_{n+1}) \\ \Rightarrow \quad & a_{n+1} = b_{n+1} \end{aligned}$$

En appliquant le principe de reccurence, (ii) est vérifiée.

□

Theorème 1.1.4. *Soit $\alpha \in \mathbb{R}$, α est un nombre rationnel si et seulement si le développement en fractions continues est simple et finie.*

Démonstration. "$\Leftarrow$" Si $[a_0, ..., a_n]$ est une fraction continue simple et finie alors c'est un nombre rationnel.

"$\Rightarrow$" Soit $\alpha \in \mathbb{Q}$.

- Si $\alpha \in \mathbb{Z}$ alors $[\alpha] = \alpha$.
- Si $\alpha \notin \mathbb{Z}$ alors $\alpha = \frac{p}{q}$ avec PGCD$p, q) = 1$ et $q \geq 1$.
  On écrit l'algorithme d'Euclide de la din de p par q.

$$\begin{array}{lll} p = a_0 q + q_1 & a_0 = E\left(\frac{p}{q}\right) & 0 < q_1 < q \\ q = a_1 q_1 + q_2 & a_1 = E\left(\frac{q}{q_1}\right) & 0 < q_2 < q_1 \\ \vdots & \vdots & \vdots \\ a_{n-2} = a_{n-1} q_{n-1} + q_n & & 0 < q_n < q_{n+1} \\ a_{n+1} = a_n q_n & & \end{array}$$

$$\frac{p}{q} = a_0 + \frac{q_1}{q}, \frac{q_1}{q} = a_1 + \frac{q_2}{q_1}, ..., \frac{q_{n-1}}{q_n} = a_n$$

$$\frac{p}{q} = [a_0, a_1, ..., a_n]$$

$a_0, ..., a_n$ sont les quotients successifs dans l'algorithme d'Euclide.

□

Développement d'un nombre réel irrationnel en fractions continues

Theorème 1.1.5. *1) Tout nombre réel irrationnel est représenté de manière unique par une fraction continue simple infinie.*

2) Soit α un nombre réel irrationnel tel que :

$$\alpha = [a_0, a_1, ..., a_n, ...]$$

Soit $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$ la suite des réduites, associée à la suite (a_i). Alonrs on a :

1) $\alpha = \lim\limits_{n\to+\infty} \dfrac{p_n}{q_n}$

2) $|\alpha - \frac{p_n}{q_n}| < \frac{1}{q_n q_{n-1}} < \frac{1}{q_n^2}$, $n \geq 1$

On dit que $\frac{p_n}{q_n}$ est la nième convergente à α.

Démonstration. i) Soit $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. On a : $\alpha = E(\alpha) + \{a\}$ où $E(\alpha)$ est la partie entière de α et $0 < \{a\} < 1$ représente la partie fractionnaire de α. On pose $a_0 = E(\alpha) \in \mathbb{Z}$ et $\{a\} = \frac{1}{\alpha_1}$, $\alpha_1 \in \mathbb{R}$.et $a_1 > 1$. Alors on a :

$$\alpha = a_0 + \frac{1}{\alpha_1} \text{ avec } \alpha_1 \in \mathbb{R},\ \alpha_1 > 1$$

$$\alpha_1 = a_1 + \frac{1}{\alpha_2} \text{ avec } \alpha_2 \in \mathbb{R},\ \alpha_2 > 1$$

Ainsi, on définit une suite $(a_i)_{i\in\mathbb{N}}$ vérifiant :

$$a_1 \geq 1 \text{ pour tout } i \geq 1$$

Soit $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$ la suite des réduites asociée à la suite $(a_i)_{i\in\mathbb{N}}$. D'après la **Proposition 1.1.2.**, la suite $\left(\frac{p_n}{q_n}\right)$ converge.
On a :

$$a_0 < \alpha < a_0 + \frac{1}{a_1} \Rightarrow \frac{p_0}{q_0} < \alpha < \frac{p_1}{q_1}$$

On peut montrer par reccurence que $\forall n \in \mathbb{N}$, on a :

$$\frac{p_{2n}}{q_{2n}} < \alpha < \frac{p_{2n+1}}{q_{2n+1}}$$

Les deux suites $\left(\frac{p_{2n}}{q_{2n}}\right)_{n\in\mathbb{N}}$ et $\left(\frac{p_{2n+1}}{q_{2n+1}}\right)_{n\in\mathbb{N}}$ convergent vers une même limite. D'après le théorème des gendarmes :

$$\lim_{n\to+\infty} \frac{p_n}{q_n} = \alpha$$

ii)

$$\left|\alpha - \frac{p_n}{q_n}\right| < \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| = \left|\frac{p_n q_{n+1} - p_{n+1} q_n}{q_n q_{n+1}}\right| = \frac{1}{q_n q_{n+1}}$$

et

$$\frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2} \text{ car } q_{n+1} > q_n$$

□

Corollaire. *Soit α un nombre réel irrationnel. Alors l'un des convergent $\frac{p_n}{q_n}$ ou $\frac{p_{n+1}}{q_{n+1}}$ vérifie :*

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{2q^2 k} \text{ avec } k = \{n, n+1\}$$

Démonstration. Pour tout $k \in \mathbb{N}$, on a :

$$\frac{p_{2k}}{q_{2k}} < \alpha < \frac{p_{2k+1}}{q_{2k+1}}$$

$$\forall n \in \mathbb{N}, \left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| = \left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| \leq \frac{1}{q_n q_{n+1}}$$

car $|p_n q_{n+1} - q_n p_{n+1}| \leq 1$. Or on a : $q_{n+1} > q_n$ pour $n \geq 1$ donc :

$$\frac{1}{q_n q_{n+1}} < \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2}$$

donc :

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2} \text{ ou } \left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| < \frac{1}{2q_{n+1}^2}$$

Si $n = 0$ et $q_1 = q_0 = 1 \Rightarrow a_1 = 1$. Dans ce cas : $\alpha = [a_0, 1, ...]$

$$\frac{p_1}{q_1} - \alpha = \frac{a_0 + 1}{1} - \alpha = 1 - \frac{1}{2} < \frac{1}{2}$$

Donc on a :

$$\left|\frac{p_1}{q_1} - \alpha\right| < \frac{1}{2q_1}$$

□

Theorème 1.1.6 (Lagrange). *Soit α un nombre irrationnel. Soit $\left(\frac{p_n}{q_n}\right)$ le nième convergeant ç α. Soient a, b des entiers premiers entre eux et $1 \leq b \leq q_n$ alors :*

$$\left|\alpha - \frac{a}{b}\right| \geq \left|\alpha - \frac{p_n}{q_n}\right|$$

C'est-à-dire $\frac{p_n}{q_n}$ est le nombre rationnel de dénominateur inférieur ou égale à q_n le plus proche de α.

Démonstration. Considérons le système d'inconnues x et y :

$$\begin{cases} p_n x + p_{n+1} y = a \\ q_n x + q_{n+1} y = b \end{cases} \qquad \begin{pmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

Il admet une solution unique car $\begin{vmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{vmatrix} = (-1)^n$.

$$x = (-1)^n(aq_{n+1} - bp_{n+1}),\ y = (-1)^n(bp_n - aq_n)$$

Notons que $x \neq 0$ (sinon $q_{n+1}|bp_{n=1}$ or $\mathrm{PGCD}(p_{n+1}, q_{n+1}) = 1$ donc $q_{n+1}|b$ or $b < q_n$ donc $x \neq 0$). Si y est nul, on a : $bp_n - q_a n$ donc $\frac{a}{b} = \frac{p_n}{q_n}$.

Dans ce cas :

$$\left|\alpha - \frac{a}{b}\right| = \left|\alpha - \frac{p_n}{q_n}\right|$$

Le théorème est, dans ce cas, vérifiée.

Si $y \neq 0$, comme $x \neq 0$, x et y sont de signe opposée, en effet :

- Si $y < 0$, on a $q_n x = b - q_{n+1} y > 0$. Donc : $x > 0$.
- Si $y > 0$, l'hypothèse nous dit : $b < q_n < q_{n+1} \Rightarrow b < yq_{n+1} \Rightarrow q_n = 0 \Rightarrow x = 0$.

D'autre part,

$$\frac{p_n}{q_n} < \alpha < \frac{p_{n+1}}{q_{n+1}}$$

Donc : $q_n\alpha - p_n$ et $q_{n+1}\alpha - p_{n+1}$ sont de signes opposés. D'où : $x(q_n\alpha - p_n)$ et $y(q_{n+1}\alpha - p_{n+1})$ sont de même signe : Donc :

$$|b\alpha - a| = |(q_x + q_{n+1}y\alpha - (q_n x + q_{n+1} y| = |x(q_n\alpha - p_n + y(q_{n+1}\alpha - p_{n+1})|$$

$$= |x(q_n\alpha - p_n)| + |y(q_{n+1}\alpha - p_{n+1}| \geq |x(q_n\alpha - p_n)| \geq |q_n\alpha - p_n|$$

$$b\left|\alpha - \frac{a}{b}\right| \geq q_n\left|\alpha - \frac{p_n}{q_n}\right|$$

Comme $b < q_n$ par hypothèse, on a :

$$\left|\alpha - \frac{a}{b}\right| \geq \left|\alpha - \frac{p_n}{q_n}\right|$$

□

1.2 Cas des nombres réels quadratiques

Définition 1.2.1. Un nombre réel α irrationnel est dit quadratique si α vérifie une équation du second degré à coefficients entiers :

$$ax^2 + bx + c \qquad a, b, c \in \mathbb{Z}$$

Remarque. 1) Si a est nule alors α serait rationnel ($b\alpha + c = 0$).

2) Le discriminants $\Delta = b^2 - 4ac \geq 0$ puisque α est une racine réel de $ax^2 + bx + c$. Les racines sont $\frac{-b-\sqrt{\Delta}}{2a}$ et $\frac{-b+\sqrt{\Delta}}{2a}$. Comme $\alpha \notin \mathbb{Q}$, $\sqrt{\Delta} \notin \mathbb{Q}$ donc Δ n'est pas un carré d'entiers.

Lemme 1.2.1. *Soit α un nombre réel. Soit β un nombre réel tel que :*

$$\alpha = \frac{a'\beta + b'}{c'\beta + d'} \text{ avec } a', b', c', d' \in \mathbb{Z} \text{ vérifiant } a'd' - b'c' = \pm 1$$

Alors on a :

1) α est quadratique si et seulement si β est quadratique.

2) si α est racine de $ax^2 + bx + c = 0$ alors β racine de l'équation $Ax^2 + Bx + C = 0$ où :

$$\begin{aligned} A &= aa'^2 + ba'c' + cc'^2 \\ B &= 2aa'b + b(a'd' + b'c') + 2c'cd' \\ C &= ab'^2 + bb'd' + cd'^2 \end{aligned}$$

De plus $B^2 - 4AC = b^2 - 4ac$.

Définition 1.2.2. Une fraction continue infinie $[a_0, a_1, ..., a_n, ...]$ est dite périodique s'il existe un entier $l > 0$ et un entier $k > 0$ tel que :

$$a_{k'} = a_{k'+l} \text{ pour tout } k' = k$$

Si on pose $n = l + k$, la fraction s'écrit :

$$[a_0, ..., a_k, a_{k+1}, ..., a_n, a_{k+1}, ...]$$

On note cette fraction :

$$[a_0, ..., a_k, \overline{a_{k+1}, ..., a_n}]$$

La longueur de la période est $n - k = l$.

Theorème 1.2.2. *La fraction continue représentant un nombre réel α est périodique si et seulement si α est quadratique.*

Démonstration. Supposons que α est représenté par une fraction continue périodique :

$$\alpha = [a_0, ..., a_k, \overline{a_{k+1}, ..., a_n}]$$

On pose $\alpha_{k+1} = [\overline{a_{k+1}, ..., a_n}]$

$$\alpha_{k+1} = [a_{k+1}, ..., a_n, a_{k+1}, ...]$$

Soit $\left(\frac{p'_i}{q'_i}\right)_{n\in\mathbb{N}}$ la suite des réduites associées à la suite $(a_i)_{i\geq k+1}$:

$$[a_{k+1}, ..., a_n] = \frac{p'_{n-k} - 1}{q'_{n-k} - 1}$$

$$[a_{k+1}, ..., a_{n-1}] = \frac{p'_{n-k-2}}{q'_{n-k-2}}$$

D'après la **Proposition 1.1.1.** :

$$\alpha_{k+1} = \frac{\alpha_{k+1}p'_{n-k-1} + p'_{n-k-2}}{\alpha_{k+1}q'_{n-k-1} + q'_{n-k-2}}$$

Donc :

$$a_{k+1}^2 q'_{n-k-1} + \alpha_{k+1}(q'_{n-k-2} - p'_{n-k-1}) - p'_{n-k-2} = 0$$

$q'_{n-k-1} \neq 0$ donc α_{k+1} est quadratique. On a :

$$\alpha = [a_0, ..., a_n, a_{k+1}, ...] = \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}}$$

$$\text{où } \left(\frac{p_k}{q_k}\right) \text{ la suite des réduits associées à la suite } (a_i)_{i\in\mathbb{N}}$$

Or on a $p_k q_{k-1} + q_k p_{k-1} = \pm 1$. Donc d'après le lemme précédent, α est quadratique.

Réciproquement, supposons que α est quadratique (racine de $ax^2 + bx + c = 0$). On écrit le développement en fraction cotninue de α.

$$\alpha = [a_0, a_1, ..., a_n]$$

Donc :

$$\alpha = [a_0, ..., a_{n-1}, \alpha_n]$$

Donc :

$$\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}$$

où $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$ est la suites des réduites associée à la suite $(a_n)_{n\in\mathbb{N}}$.

Comme $q_{n-2}p_{n-1} - q_{n-1}p_{n-2} = \pm 1$, d'après le lemme précédent α_n est périodique. Ecrivons l'équation de α :

$$A_n\alpha_n^2 + B_n\alpha_n + C_n = 0$$

avec :

$$\begin{aligned} A_n &= ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2 \\ B_n &= 2ap_{n-1}p_{n-2} + b(p_{n-1}q_{n-2} + q_{n-1}p_{n-2}) + 2cq_{n-1}q_{n-2} \\ C_n &= qp_{n-2}^2 + bp_{n-2}q_{n-2} + cq_{n-2}^2 = A_{n-1} \end{aligned}$$

D'après le **Lemme 1.2.1.**, on a : $B_n^2 - 4A_nC_n = b^2 - 4ac$. Montrons que $\{(A_n, B_n, C_n),\ n \in \mathbb{N}\}$ est finie : cet ensemble sera donc majorée. Posons :

$$\delta_n = \frac{p_{n-1}}{q_{n-1}} - \alpha$$

Or :

$$|\delta_n| \leq \frac{1}{q_{n-1}^2} \text{ (d'après le } \textbf{Théorème 1.1.5.}\text{)}$$

Donc :

$$|A_n| \leq |q_{n-1}^2[\underbrace{a\alpha^2 + b\alpha + c}_{0} + a\delta_n^2 + 2a\alpha\delta_n + b\delta_n]| \leq |a| + |2a\alpha| + |b|$$

Comme $C_n = A_{n-1}$ donc la suite $(|C_n|)$ est majorée. Or on a :

$$B_n^2 = 4A_nC_n + b^2 - 4ac$$

Donc la suite $(|B_n|)_{n\in\mathbb{N}}$ est majorée. Donc : $\{(A_n, B_n, C_n),\ n \in \mathbb{N}\}$ est finie. Donc il existe $n_1, n_2, n_3 \in \mathbb{N}$, $n_1 < n_2 < n_3$ tel que :

$$A_{n_1} = A_{n_2} = A_{n_3}$$

$$B_{n_1} = B_{n_2} = B_{n_3}$$

$$C_{n_1} = C_{n_2} = C_{n_3}$$

On pose $A = A_{n_1} = A_{n_2} = A_{n_3}$, $B = B_{n_1} = B_{n_2} = B_{n_3}$ et $C = C_{n_1} = C_{n_2} = C_{n_3}$.

Or $\alpha_{n+1}, \alpha_{n+2}, \alpha_{n+3}$ sont racines de l'équation $Ax^2 + Bx + C = 0$. Donc deux d'entre elles (parmi ces racines) sont égales. Par exemple, si $a_{n_1} = a_{n_2}$ alors :

$$[a_{n_1}, ...] = [a_{n_2}, ...]$$

Donc $a_{n_1} = a_{n_2}$, $a_{n_1+1} = a_{n_2+1}$. Donc :

$$\alpha = [a_0, ..., a_{n_1-1}, a_{n_1}, ..., a_{n_2-1}, a_{n_1}, ...] = [a_0, ..., a_{n_1-1}, \overline{a_{n_1}, ..., a_{n_2-1}}]$$

Donc : α est périodique. □

Définition 1.2.3. Soit α un nombre réel quadratique (racine de $ax^2 + bx + c = 0$). L'autre racine qu'on note $\overline{\alpha}^{\mathbb{R}}$ s'appelle le conjugé de α.

Si $\alpha = \frac{-b+\sqrt{\Delta}}{2a}$ alors $\overline{\alpha}^{\mathbb{R}} = \frac{-b-\sqrt{\Delta}}{2a}$.

Attention :. ici le conjugué n'est pas le conjugué au sens complexe. On note $\overline{\alpha}^{\mathbb{R}}$ le conjugué.

Remarque.

$$ax^2 + bx + c = a(x - \alpha)(x - \overline{\alpha}) \Rightarrow \alpha\overline{\alpha} = \frac{-c}{a} \text{ et } a + \overline{\alpha} = \frac{-b}{a}$$

Définition 1.2.4. Soit α un nombre réel quadratique. On dit que α est purement périodique si la décomposition de α en fraction continue est de la forme :

$$\alpha = [\overline{a_0, ..., a_{l-1}}]$$

c'est-à-dire la période commence à partir du premier coefficient.

Remarque. Si $\alpha = [\overline{a_0, ..., a_{l-1}}]$, on a :

$$a_{l+n} = a_n \text{ pour tout } n \in \mathbb{N}$$

Si on note $\alpha_n = [a_n, a_{n+1}, ...]$. On a : $\alpha_{n+l} = \alpha_n$ pour tout $n \in \mathbb{N}$ ($\alpha_l = \alpha_0 = \alpha$).

On a : $a_0 = a_l \geq 1$ donc $\alpha \geq 1$.

On a aussi :

$$\alpha = [a_0, ..., a_{l-1}, \alpha] = \frac{p_{l-1}\alpha + p_{l-2}}{q_{l-1}\alpha + q_{l-2}}$$

où $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$ est la $n$ième convergente à α donc vérifie $q_{l-1}\alpha^2 + (q_{l-2} - p_{l-1})\alpha + p_{l-2} = 0$. Donc : $\alpha\overline{\alpha} = -\frac{p_{l-2}}{q_{l-1}} < 0$. Comme $\alpha > 1$, $\overline{\alpha} < 0$. Conclusion : si α est purement périodique : $\alpha > 1$ et $\overline{\alpha} < 0$.

Lemme 1.2.3. *Soit $(a_i)_{i\in\mathbb{N}}$ une suite d'entiers ≥ 1 et soit $\left(\frac{p_i}{q_i}\right)_{i\in\mathbb{N}}$ la suite des réduites associée à la suite $(a_i)_{i\in\mathbb{N}}$. Alors $\forall k > 1$, on a :*

$$[a_k, ..., a_0] = \frac{p_k}{p_{k-1}}$$

$$[a_k, ..., a_1] = \frac{q_k}{q_{k-1}}$$

Proposition 1.2.4. *Soit α un nombre réel purement périodique dont le développement en fraction continue s'écrit :*

$$\alpha = [\overline{a_0, ..., a_{l-1}}]$$

Alors :

$$-\frac{1}{\overline{\alpha}} = [\overline{a_{l-1}, ..., a_0}]$$

Démonstration. On a :

$$\alpha = [a_0, ..., a_{l-1}, \alpha]$$

Donc α vérifie l'équation :

$$q_{l-1}\alpha^2 + (q_{l-2} - p_{l-1}\alpha + p_{l-2} = 0 \qquad (*)$$

Posons :

$$\alpha' = [\overline{a_{l-1}, ..., a_0}] = [a_{l-1}, ..., a_0, \alpha]$$

Or d'après le **Lemme 1.2.3.**, on a :

$$[a_{l-1}, ..., a_0] = \frac{p_{l-1}}{p_{l-2}}$$

$$[a_{l-1}, ..., a_1] = \frac{q_{l-1}}{q_{l-2}}$$

D'où $[a_{l-1}, ..., a_0, \alpha'] = \frac{p_{l-1}\alpha' + q_{l-1}}{p_{l-2}\alpha' + q_{l-2}}$ d'après la **Proposition 1.1.1.**. Donc :

$$\alpha' = \frac{p_{l-1}\alpha' + q_{l-1}}{p_{l-2}\alpha' + q_{l-2}}$$

Donc :

$$p_{l-2}\alpha'^2 + (q_{l-2} - p_{l-1})\alpha' + q_{l-1} = 0$$

Donc :

$$-p_{l-2} + (-q_{l-1} + p_{l-2}) \times \left(\frac{-1}{\alpha'}\right) - q_{l-1} \times \left(\frac{-1}{\alpha'}\right)^2 = 0$$

Donc : $-\frac{1}{\alpha}$ vérifie la même équation que α (voir $(*)$). D'où $-\frac{1}{\alpha'} = \alpha$ ou $-\frac{1}{\alpha} = \overline{\alpha}$. Or $-\frac{1}{\alpha} < 0$ donc $-\frac{1}{\alpha'} = \overline{\alpha}$ donc $\alpha' = -\frac{1}{\overline{\alpha}}$. D'où :

$$-\frac{1}{\overline{\alpha}} = [\overline{a_{l-1}, .., a_0}]$$

□

Theorème 1.2.5 (Caractérisation des réels purement périodiques - Evariste Galois)**.** *Soit α un nombre réel quadratique alors α est purement périodique $\Leftrightarrow \alpha > 1$ et $-1 < \overline{\alpha} < 0$*

Démonstration. ($\Rightarrow$) Si α est périodique, $\alpha = [a_0, ..., a_{l-1}]$. On a $\alpha > 1$ et d'après la **Proposition 1.2.4.**, on a :

$$-\frac{1}{\overline{\alpha}} = [\overline{a_{l-1}, ..., a_0}] \text{ donc } -\frac{1}{\overline{\alpha}} > 1$$

Donc :

$$-1 < \overline{\alpha} < 0$$

($\Leftrightarrow$) Supposons que α est quadratique et :

$$\alpha > 1,\ -1 < \overline{\alpha} < 0$$

Comme α est quadratique, son développement en fraction continue est périodique.

$$\alpha = [a_0, ..., \overline{a_k, ..., a_{k+l-1}}]$$

Posons :

$$\alpha_n = [a_n, a_{n+1}, ...],\ n \in \mathbb{N}$$

On a : $\alpha = \frac{1}{\alpha}$. Donc : $\frac{1}{\alpha_1} = \alpha - a_0$. Donc :

$$-\frac{1}{\overline{\alpha_1}} = \overline{a_0 - \alpha}^{\mathbb{R}} = \alpha_0 - \overline{\alpha}$$

Comme $-1 < \overline{\alpha} < 0$, on a : $a_0 < -\frac{1}{\alpha_1} < a_0 + 1$. Donc :

$$E\left(-\frac{1}{\alpha_1}\right) = a_0$$

On montre par reccurence que $E\left(-\frac{1}{\overline{\alpha_{n+1}}}\right) = a_n$. C'est vrai pour $n = 0$. Supposons que $a_{n-1} = E\left(-\frac{1}{\overline{\alpha_n}}\right)$. Or on a : $\alpha_n = a_n + \frac{1}{\alpha_n}$. Donc : $-\frac{1}{\overline{\alpha_{n+1}}} = a_n - \overline{\alpha_n}$ or $-1 < \overline{\alpha_{n+1}} < 0$ car $E\left(-\frac{1}{\overline{\alpha_n}}\right) \geq 1$. Donc :

$$a_n < -\frac{1}{\overline{\alpha_n}} < a_n + 1 \Rightarrow E\left(-\frac{1}{\overline{\alpha_{n+1}}}\right) = a_n$$

Comme $\alpha_{k+1} = \alpha_{k+l+1}$ (car α est périodique et la longueur de la période est l). Donc : $\overline{\alpha_{k+1}}^{\mathbb{R}} = \overline{\alpha_{k+l+1}}^{\mathbb{R}} \Rightarrow E\left(-\frac{1}{\overline{\alpha_{k+1}}}\right) = E\left(-\frac{1}{\overline{\alpha_{k+l+1}}}\right)$. Donc $a_k = a_{k+l}$. On en déduit que $\alpha_1 = \alpha_{l+1}$. D'où $E\left(-\frac{1}{\overline{\alpha_1}}\right) = E\left(-\frac{1}{\overline{\alpha_{l+1}}}\right)$. D'où : $a_0 = a_l$. Donc $a_k = a_{k+l}$, $\forall k \in \mathbb{N}$. Donc : $\alpha = [\overline{a_0, ..., a_{l-1}}]$, α est purement périodique.

□

Theorème 1.2.6. *Soit d un entier ≥ 1, non carré parfait. Soit l la longueur d'une période minimale de la fraction continue de $\sqrt{d}$. Alors on a :*

$$\sqrt{d} = [a_0, \overline{a_1, ..., a_l}]$$

où

$$E(\sqrt{d}) = a_0 \text{ et } a_l = 2a_0, a_{l-i} = a_i,\ \forall i \in \mathbb{N}^*$$

Démonstration. On pose $a_0 = E(\sqrt{d})$ et $\alpha = a_0 + \sqrt{d}$. On a $1 < \alpha$ et $\overline{\alpha} = a_0 - \sqrt{d}$ donc $-1 < \overline{\alpha} < 0$. Donc d'après le **Théorème 1.2.5.** α est purement périodique. Or : $E(\alpha) = 2a_0$ donc $\alpha = \overline{[2a_0, ..., a_{l'-1}]}$. D'après la **Proposition 1.2.4.**, on a :

$$-\frac{1}{\overline{\alpha}} = \overline{[a_{l'-1}, ..., 2a_0]}$$

Or :

$$-\frac{1}{\overline{\alpha}} = -\frac{1}{a_0 - \sqrt{d}} = \frac{1}{\sqrt{d} - a_0}$$

Or :

$$\sqrt{d} = \alpha - a_0 = 2a_0 + \frac{1}{\overline{[a_1, ..., a_{l'-1}, 2a_0]}} - a_0 = \overline{[a_0, a_1, ..., a_{l'-1}, 2a_0]}$$

Donc : $l' = l$. D'où :

$$-\frac{1}{\overline{\alpha}} = \overline{[a_1, ..., a_{l-1}, 2a_0]}$$

or :

$$-\frac{1}{\overline{\alpha}} = \overline{[a_{l-1}, ..., 2a_0]}$$

Donc : $\forall i \in \mathbb{N}^*$, $a_i = a_{l+i}$. □

Proposition 1.2.7. *Soit d un entier non carré parfait, $\sqrt{d} = [a_0, \overline{a_1, ..., a_l}]$ avec $a_l = 2a_0$ et $a_{l-1} = a_i$ pour $1 \leq i \leq l-1$ (l la période minimale).*

Posons $\alpha = \sqrt{d}$, $\alpha_n = [a_n, a_{n+1}, ...] = \frac{b_n + \sqrt{d}}{c_n}$ où $b_n, c_n \in \mathbb{Z}$.

On désigne par $\frac{p_n}{q_n}$ la nième convergente à $\alpha = \sqrt{d}$. Alors on a :

1) $p_{n-1}^2 - dq_{n-1}^2 = (-1)^n c_n$ (Equation de Pell-Fermat)

2) $c_n = 1 \Leftrightarrow \exists k \in \mathbb{N}^*$ tel que $n = kl$.

Démonstration. 1) On a :

$$\alpha = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}} \text{ pour } n \geq 2 \qquad (*)$$

$$\alpha_n = \frac{b_n + \sqrt{d}}{c_n}$$

$(*)$ devient :

$$(*) \Rightarrow \underbrace{\sqrt{d}}_{\notin \mathbb{Q}} \underbrace{\left(q_{n-1}\frac{b_n}{c_n} + q_{n-2} \right)}_{\in \mathbb{Q}} = \underbrace{\frac{p_{n-1}}{c_n}}_{\in \mathbb{Q}} \sqrt{d} + \underbrace{\frac{p_{n-1} + b_n}{c_n}}_{\in \mathbb{Q}} + p_{n-2}$$

$$\Rightarrow \underbrace{\sqrt{d}}_{\notin \mathbb{Q}} \underbrace{\left(q_{n-1}\frac{b_n}{c_n} + q_{n-2} - \frac{p_{n-1}}{c_n} \right)}_{\in \mathbb{Q}} = \underbrace{\frac{p_{n-1}b_n}{c_n}}_{\in \mathbb{Q}} - p_{n-2} - \underbrace{\frac{q_{n-1}d}{c_n}}_{\in \mathbb{Q}}$$

$$\begin{cases} q_{n-1}b_n + q_{n-2}c_n = p_{n-1} \\ p_{n-1}b_n + p_{n-2}c_n = q_{n-1}d \end{cases}$$

D'où :

$$\begin{aligned} p_{n-1}^2 - dq_{n-1}^2 &= p_{n-1}(q_{n-1}b_n + q_{n-2}c_n) - q_{n-1}(p_{n-1}b_n + p_{n-2}c_n) \\ &= c_n(p_{n-1}q_{n-2} - q_{n-1}p_{n-2} = (-1)^n c_n \end{aligned}$$

2) $\Leftarrow$:

$$\alpha_l = a_l + \frac{1}{\alpha_{l+1}} = a_l + \frac{1}{\alpha_1} \text{ (car } l \text{ la période de } \sqrt{d}$$

$$= 2a_0 + \frac{1}{\alpha_1} = 2a_0 + \frac{1}{\sqrt{d} - a_0}$$

Or : $\alpha_l = \frac{b_l+\sqrt{d}}{c_l} = a_0 + \sqrt{d} \Rightarrow b_l = a_0, c_l = 1$. Par périodicité, on a :

$$\forall k \in \mathbb{N}^*, \alpha_{kl} = \alpha_l = a_0 + \sqrt{d}$$

Or : $\alpha_{kl} = \frac{b_{kl}+\sqrt{d}}{c_{kl}}$. Donc : $c_{kl} = 1$.

$\Rightarrow$: Supposons que $c_n = 1$ donc $\alpha_n = b_n + \sqrt{d}$ d'où $\overline{\alpha_n} = b_n - \sqrt{d}$. Or :

$$\alpha_n = [\overline{a_n, a_{n+1}, ..., a_l, a_1, ..., a_{n-1}}]$$

α_n est purement périodique. D'après le **Théorème 1.2.5.**, $-1 < \overline{\alpha_n} < 0$. Donc $-1 < b_n - \sqrt{d} < 0$ et $b_n < \sqrt{d} < b_n + 1$.
Donc : $b_n = E(\sqrt{d}) = a_0$, $\alpha_n = a_0 + \sqrt{d} = \alpha_l$ et l étant la période minimale de la fraction continue donc $l|n$.

□

Corollaire. *Soit d un entier non carré parfait, l la période minimal de $\sqrt{d}$. Alors on a :*

1) Si l est pair, pour tout $k \in \mathbb{N}^*$, (p_{kl-1}, q_{kl-1}) est une solution de l'équation appelée équation de Pell-Fermat : $x^2 + dy^2 = 1$, $x, y \in \mathbb{Z}$.

2) Si l est impair, pour tout $k \in \mathbb{N}^*$, $(p_{(2k+1)l-1}, q_{(2k+1)l-1})$ est une solution de l'équation $x^2 - dy^2 = -1$, $x, y \in \mathbb{Z}$ et (p_{2kl-1}, q_{2kl-1}) est une solution de l'équation de Pell-Fermat.

1.3 Equation de Pell-Fermat

1.3.1 Structure de $\mathbb{Z}[\sqrt{d}]$

Notation. Soit d un entier non carrée. On note :

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d},\ a \in \mathbb{Z}, b \in \mathbb{Z}\}$$

Remarque. $a + b\sqrt{d} = a' + b'\sqrt{d}$ avec $a, b, a', b' \in \mathbb{Z}$ car $a - a' = (b' - b)\sqrt{d}$. Si $b \neq b'$, on aura : $\sqrt{d} = \frac{a-a'}{b'-b}$. Or $\sqrt{d} \notin \mathbb{Q}$. Donc $b = b'$ et $a = a'$. Il y a unicité de l'écriture dans $\mathbb{Z}[\sqrt{d}]$.

Proposition 1.3.1. $(\mathbb{Z}[\sqrt{d}], +, \times)$ *est un sous-anneau de* $\mathbb{R}$.

Démonstration. $*$ On démontre que $(\mathbb{Z}[\sqrt{d}], +)$ est un ensemble stable. Soient $x, x' \in \mathbb{Z}[\sqrt{d}]$. Il existe $a, b, a', b' \in \mathbb{Z}$ tel que :

$$x = a + b\sqrt{d}$$

$$x' = a' + b'\sqrt{d}$$

On décrit :

$$(x - x') = a - a' + (b - b')\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$$

Or $a - a' \in \mathbb{Z}$ et $b - b' \in \mathbb{Z}$ donc $x - x' \in \mathbb{Z}[\sqrt{d}]$. Donc $(\mathbb{Z}[\sqrt{d}], +)$ est un sous-groupe de $(\mathbb{R}, +)$.

*

$$x \times x' = (a+b\sqrt{d})(a'+b'\sqrt{d}) = aa' + bb'd + ab'\sqrt{d} + ba'\sqrt{d} = \underbrace{aa'+bb'd}_{\in\mathbb{Z}} + \underbrace{(ba'+b'a)}_{\in\mathbb{Z}}\sqrt{d}$$

Donc : $x.x' \in \mathbb{Z}[\sqrt{d}]$

Donc : $(\mathbb{Z}[\sqrt{d}], +, \times)$ est un sous-anneau de $\mathbb{R}$. □

Remarque. $(\mathbb{Z}[\sqrt{d}], \times)$ n'est pas un groupe car $3 \in \mathbb{Z}[\sqrt{d}]$ mais $\frac{1}{3} \notin \mathbb{Z}[\sqrt{d}]$ car $\frac{1}{3} \notin \mathbb{Z}$.

Notation. Soit $x = a + b\sqrt{d}$. On note $\overline{x} = a - b\sqrt{d}$, le conjugué de x et on note la norme de x, $N(x) = x\overline{x} = a^2 - db^2 \in \mathbb{Z}$.

Lemme 1.3.2. *$\forall x, y \in \mathbb{Z}[\sqrt{d}]$, on a :*

$$N(xy) = N(x)N(y)$$

(la norme N est multiplicative).

Démonstration. $x = a + b\sqrt{d}$, $y = a' + b'\sqrt{d}$ avec $a, a', b, b' \in \mathbb{Z}$. Donc :

$$xy = aa' + dbb' + (ab' + a'b)\sqrt{d}$$

$$\overline{xy} = aa' + dbb' - (ab' + a'b)\sqrt{d}$$

$$N(xy) = xy\overline{xy} = ((aa'+b)+dbb'+(ab'+a'b)\sqrt{d})((aa'+bb')-(a'b+b'a)\sqrt{d}) = (aa'+dbb')^2-(ab'+ab)^2$$

$$N(x)N(y) = (a^2 - db^2)(a'^2 - db'^2)$$

On vérifie alors que $N(xy) = N(x)N(y)$. □

Proposition 1.3.3. *Soit $x \in \mathbb{Z}[\sqrt{d}]$, x est inversible si et seulement si $N(x) = \pm 1$. Cela veut dire que si $x = a + b\sqrt{d}$, x est inversible $\Leftrightarrow a^2 + b^2 d = \pm 1$.*

Démonstration. ($\Rightarrow$) Soit $x \in \mathbb{Z}[\sqrt{d}]$, x est inversible dans $\mathbb{Z}[\sqrt{d}] \Leftrightarrow$ il existe $x' \in \mathbb{Z}[\sqrt{d}]$ tel que $xx' = 1$. Donc : $N(xx') = N(1) = 1$. Or $N(xx') = N(x)N(x')$. Donc : $N(x)N(x') = 1$. Donc $N(x) = \pm 1$ car $N(x), N(x') \in \mathbb{Z}$

($\Leftarrow$) Soit $x \in \mathbb{Z}[\sqrt{d}]$. Supposons que $N(x) = \pm 1$. Donc : $a^2 - db^2 = \pm 1 \Rightarrow (a + b\sqrt{d})(a - b\sqrt{d}) = \pm 1$

$$\Rightarrow \frac{1}{a + b\sqrt{d}} = \pm(a - \sqrt{d}) \in \mathbb{Z}[\sqrt{d}]$$

Donc : x est inversible dans $\mathbb{Z}[\sqrt{d}]$.

□

Remarque. Soit $x = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ alors :

1. $N(x) = 1 \Leftrightarrow a^2 - b^2 d = 1 \Leftrightarrow (a, b)$ solution de Pell-Fermat.
2. $N(x) = 1 \Leftrightarrow \frac{1}{x} = a - b\sqrt{d} = \overline{x}$
3. On a vu que l'équation de Pell-Fermat admet une infinité de solutions. Il y a donc une infinité d'éléments inversibles dans $\mathbb{Z}[\sqrt{d}]$.

1.3.2 Equation de Pell-Fermat

Définition 1.3.1. Soit d un entier > 1 non carré. On considère l'équation de Pell-Fermat (E) : $x^2 - dy^2 = 1$, $x, y \in \mathbb{Z}$. On a vu que cette équation admet une infinité de solutions. L'objet est de déterminer toutes les solutions.

Proposition 1.3.4. *Il existe une solution (x_0, y_0) de (E) vérifiant, $x_0 > 0$, $y_0 > 0$ et pour toute solution (x, y) de (E) tel que $x > 0$, $y > 0$. On a : $x + y\sqrt{d} \geq x_0 + y_0\sqrt{d}$. Cette solution (x_0, y_0) est appelée la solution fondamentale de (E).*

Démonstration. Supposons que la **Proposition 1.3.2.** est fausse : donc on peut construire une suite décroissante (α_n) avec $\alpha_n = x_0 + y_0\sqrt{d}$ et (x_0, y_0) soltuion de (E). La suite (α_n) est décroissante minorée par 0 donc elle converge dans $\mathbb{R}$ et $\lim \alpha_n \neq 0$. Donc $\lim\limits_{n\to+\infty} \dfrac{\alpha_n}{\alpha_{n+1}} = 1$. Remarquons, $\forall n$, $\frac{\alpha_n}{\alpha_{n+1}} > 1$. Or (x_0, y_0) est solution de E donc $N(x_n) = 1$ pour tout n. Donc pour tout n, α_n est inversible dans $\mathbb{Z}[\sqrt{d}]$. Donc :

$$\forall n \in \mathbb{N}, \frac{\alpha_n}{\alpha_{n+1}} \in \mathbb{Z}[\sqrt{d}]$$

et $N\left(\frac{\alpha_n}{\alpha_{n+1}}\right) = \frac{N(\alpha_n)}{N(\alpha_{n+1})} = 1$. Donc : $\frac{\alpha_n}{\alpha_{n+1}} = X_n - Y_n\sqrt{d}$ et $X_n^2 - Y_n^2 d = 1$. Comme $\frac{\alpha_n}{\alpha_{n+1}} > 1$, on a : $Y_n \neq 0$. On a : $\frac{\alpha_n}{\alpha_{n+1}} = (x_0 - y_0\sqrt{d})(x_{n+1} - y_{n+1}\sqrt{d})$. Cela vérifie $Y_n > 0$. Donc $\frac{\alpha_n}{\alpha_{n+1}} \geq \sqrt{d}$ (Absurde car $\lim \frac{\alpha_n}{\alpha_{n+1}} = 1$). □

Theorème 1.3.5. *Soit (x_0, y_0) la solution fondamentale, toute solution de (E) s'exprime en fonction de (x_0, y_0) (solution fondamentale). C'est-à-dire soit (x, y) solution de E alors il existe $m \in \mathbb{Z}$ tel que :*

$$x + y\sqrt{d} = \pm(x_0 + y_0\sqrt{d})^m$$

Démonstration. 1) Si (x, y) vérifie $x + y\sqrt{d} = (x_0 + y_0\sqrt{d})^m$, on a : $N(x + y\sqrt{d}) = N((x_0 + y_0\sqrt{d})^m) = (N(x_0 + y_0\sqrt{d})^m$. Or (x_0, y_0) solution de Pell-Fermat donc $N(x_0 + y_0\sqrt{d}) = 1$. Donc $1 = (N(x_0 + y_0\sqrt{d})^m) = N(x + y\sqrt{d})$. Donc (x, y) solution de Pell-Fermat.

2) Réciproquement, soit (x, y) une solution de (E). Soit m le plus grand entier ≥ 0 tel que :

$$(x_0 + y_0\sqrt{d})^m \leq x + y\sqrt{d}$$

(on suppose que $x > 0$, $y > 0$). Donc :

$$(x_0 + y_0\sqrt{d})^m \leq x + y\sqrt{d} \leq (x_0 + y_0\sqrt{d})^{m+1}$$

Donc :

$$1 \leq (x + y\sqrt{d})(x_0 - y_0\sqrt{d})^{-m} \leq (x_0 + y_0\sqrt{d})$$

On a $N(x_0+y_0\sqrt{d}) = 1$. Donc $(x_0+y_0\sqrt{d})^{-1} = x_0-y_0\sqrt{d}$ d'où $(x_0+y_0\sqrt{d})^{-m} = (x_0-y_0\sqrt{d})^m$ et donc $(x + y\sqrt{d})(x_0 + y_0\sqrt{d})^{-m} \in \mathbb{Z}[\sqrt{d}]$. Posons $(x + y\sqrt{d})(x_0 + y_0\sqrt{d})^{-m} = X_n - Y_n\sqrt{d}$ On a :

$$\begin{aligned} N(X_n - Y_n\sqrt{d}) &= N((x + y\sqrt{d})(x_0 + y_0\sqrt{d})^{-m}) \\ &= N(x + y\sqrt{d}) \times N(x_0 - y_0\sqrt{d}) \\ &= N(x + y\sqrt{d}) = 1 \end{aligned}$$

car (x, y) est solution de Pell-Fermat $\Rightarrow N(x_0 + y_0)^{-m} = (1)^{-m} = 1$ et (x, y) solution de Pell-Fermat. Donc (X_n, Y_n) solution de (E) et :

$$1 \leq X_n + Y_n\sqrt{d} \leq x_0 + y_0\sqrt{d}$$

Comme (x_0, y_0) est solution fondamentale, on a : $Y_n = 0$ et $X_n = 1$. Donc :

$$x_n + y_n\sqrt{d} = (x_0 + y_0\sqrt{d})^m$$

3) Soit (x, y) solution de (E) tel que $x > 0$ et $y \leq 0$ donc $(x, -y)$ est solution de E avec $x > 0, y \geq 0$. On déduit du cas précédent qu'il existe $m \in \mathbb{N}$ tel que :

$$x - y\sqrt{d} = (x_0 + y_0\sqrt{d})^m$$

d'où $x + y\sqrt{d} = (x - y\sqrt{d})^{-1} = (x_0 + y_0\sqrt{d})^{-m}$ car $N(x + y\sqrt{d}) = 1$.

4) Soit (x, y) solution de E tel que $x < 0$ et $y \leq 0$ donc $(-x, y)$ solution de E avec $-x > 0$, $-y \geq 0$. Donc il existe $m \in \mathbb{N}$ tel que $-x - y\sqrt{d} = (x_0 + y_0\sqrt{d})^{-m}$. D'où :

$$x + y\sqrt{d} = (x_0 + y_0\sqrt{d})^m$$

5) Soit (x, y) solution de E tel que $x < 0$ et $y \geq 0$, il existe $m \in \mathbb{N}$ tel que $-x + y\sqrt{d} = (x_0 + y_0\sqrt{d})^m$. On a : $-x - y\sqrt{d} = (-x + y\sqrt{d})^{-1} = (x_0 + y_0\sqrt{d})^{-m}$. Donc :

$$x + y\sqrt{d} = -(x_0 + y_0\sqrt{d})^{-m}$$

□

Proposition 1.3.6. *On note $U_d = \{x + y\sqrt{d},\ x^2 - dy^2 = 1\}$, $(U_d, \times)$ est une groupe engendré modulo $\{-1, 1\}$ par $x_0 + y_0\sqrt{d}$ (groupe monogène).*

Démonstration. $(U_d, \times)$ est un sous-groupe de $(\mathbb{R}^\times, \times)$. Soit x, y et x', y' tel que $x + y\sqrt{d} \in U_d$ et $x' + y'\sqrt{d} \in U_d$.

$$(x + y\sqrt{d})(x' + y'\sqrt{d}) \in \mathbb{Z}[\sqrt{d}]$$

Comme $N((x+y\sqrt{d})(x'+y'\sqrt{d})) = N(x+y\sqrt{d})N(x'+y'\sqrt{d} = 1$. Donc : $(x+y\sqrt{d})(x'+y'\sqrt{d}) = U_d$.

Soit $(x + y\sqrt{d}) \in U_d$, $N(x + y\sqrt{d}) = 1$, donc $\frac{1}{x+y\sqrt{d}} = x - y\sqrt{d} \in U_d$. □

Question Comment trouver la solution fondamentale de l'équation de Pell-Fermat ?

Lemme 1.3.7. *Soit $\alpha \in \mathbb{R}$ tel que*

$$\alpha = \frac{p\beta + r}{q\beta + s}$$

avec β un nombre réel ≥ 1, p, q, r, s des entiers tels que $q > s > 0$ et $ps - qr = \pm 1$. Alors $\frac{r}{s}$ et $\frac{p}{q}$ sont des convergents successifs de α.où $\frac{r}{s}$ est le $(n-1)^{ème}$ convergent de α, $\frac{p}{q}$ est le nième convergent de α et β le $(n+1)^{ème}$ quotient complet de α ($\beta = \alpha_{n+1}$).

Démonstration. On choisit le développement de $\frac{p}{q}$ en fraction continue de la forme $\frac{p}{q} = [a_0, ..., a_n]$ tel que $(-1)^{n-1} = ps - qr$. Soit $\left(\frac{p_i}{q_i}\right)_{i\in\mathbb{N}}$ la suite des réduites associés à la suite $a_0, ..., a_n$. Comme $\mathrm{PGCD}(p, q) = 1$, on a $p = p_n$ et $q = q_n$ donc $pq_{n-1} = qp_{n-1} = p_nq_{n-1} - q_np_{n-1} = (-1)^{n-1} = ps - qr \Rightarrow p(q_{n-1} - s) - q(-r + p_{n-1})$ donc $q|p(q_{n-1} - s)$ et $\mathrm{PGCD}(p, q) = 1 \Rightarrow q|q_{n-1} - s$. Comme $s \geq 0$ et $q_n > q_{n-1}$. on $q_{n-1} - s = 0$. Donc $q_{n-1} - s = 0$ et $p_{n-1} = 1$. Donc $\frac{p}{q} = \frac{p_n}{q_n}$ et $\frac{r}{s} = \frac{p_{n-1}}{q_{n-1}}$ d'où :

$$\alpha = \frac{p_n\beta + p_{n-1}}{q_n\beta + q_{n-1}} = [a, 0, ..., a_n, \beta]$$

Comme $\beta > 1$, donc β est le $(n+1)^{\text{ème}}$ quotient complet de α. □

Theorème 1.3.8 (Legendre)**.** *Soit α un nombre réel. Soient p, q deux entiers tels que* $\mathrm{PGCD}(p,q) = 1$, $q > 0$. *Si $|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$ alors $\frac{p}{q}$ est un convergent de α.*

Démonstration. Supposons que $|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$ donc p, q vérifient les hypothèses du **Théorème 1.3.6.** Posons : $\alpha - \frac{p}{q} = \varepsilon\frac{\theta}{q^2}$ avec $\varepsilon = \begin{cases} 1 \text{ si } \alpha \geq \frac{p}{q} \\ 0 \text{ si } \alpha < \frac{p}{q} \end{cases}$. Puisque $|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$, on a $0 < \theta < \frac{1}{2}$. On choisit un développment en fraction continue de $\frac{p}{q}$ tel que $\frac{p}{q} = [a_0, ..., a_n]$ avec $(-1)^n = \varepsilon$. Soit $\left(\frac{p_i}{q_i}\right)$ la suite des réduites associées à la suites $a_0, ..., a_n$ donc $p = p_n$ et $q = q_n$. Soit β le nombre réel tel que :

$$\alpha = \frac{\beta p_n - p_{n-1}}{\beta q_n - q_{n-1}}$$

On a :

$$\varepsilon\frac{\theta}{q_n^2} = \varepsilon\frac{\theta}{q^2} = \alpha - \frac{p}{q} = \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n+1}} - \frac{p_n}{q_n}$$

Si l'on réduit au même dénominateur :

$$\frac{\beta p_n + p_{n+1}}{\beta q_n + q_{n+1}} - \frac{p_n}{q_n} = \frac{q_n p_{n-1} + p_n q_{n-1}}{q_n(\beta q_n + q_n + 1)} = \frac{(-1)^n}{q_n(\beta q_n + q_{n+1}} = \frac{\varepsilon}{q_n(\beta q_n + q_{n-1}}$$

Cela entraîne que $\theta = \frac{q_n}{\beta q_n + q_{n-1}} \Rightarrow \underbrace{\frac{1}{\theta}}_{>2} - \underbrace{\frac{q_{n+1}}{q_n}}_{>1} > 1$. Donc $\beta > 1$. D'après le **Lemme 1.3.5.**, $\frac{p}{q}$ est une convergent de α. □

Corollaire. *Soit d un entier > 4 non carré. Alors :*

1) *Si (x, y) est solution de l'équation de Pell-Fermat $(E) : x^2 - dy^2 = 1$, $x > 0$, $y > 0$ alors $\frac{x}{y}$ est un convergent de $\sqrt{d}$.*
2) *Soit l la période (minimale) de $\sqrt{d}$. On note $\frac{p_n}{q_n}$ le nième convergent de $\sqrt{d}$. Si l paire, (p_{l-1}, q_{l-1}) est solution fondamentale de Pell-Fermat. Si l est impaire, (p_{2l-1}, q_{2l-1}) est la solution fondamentale de Pell-Fermat.*

Démonstration. 1) Soit (x, y) solution de (E) avec $\mathrm{PGCD}(x, y) = 1$, $x > 0$, $y > 0$. On a $x^2 - dy^2 = 1$. Donc : $|x - y\sqrt{d}| = \frac{1}{x + y\sqrt{d}}$. Donc :

$$\left|\frac{x}{y} - \sqrt{d}\right| = \frac{1}{y|x + y\sqrt{d}|} < \frac{1}{y^2\sqrt{d}}$$

car $x > 0$, $y > 0$. Comme $d > 4$, on a :

$$\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{2y^2}$$

Donc : d'après le **Théorème 1.3.6.**, $\frac{x}{y}$ est un convergent $\sqrt{d}$.

2) Soit l la période du développement en fractions continues de $\sqrt{d}$, si l est pair, on a vu que (p_{l-1}, q_{l-1}) vérifie l'équation $x^2 - dy^2 = 1$ (d'après le dernier **Corollaire** de la **Section 1.2.**). Si $0 < i < l - 1$, (p_i, q_i) n'est pas soltuion de Pell-Fermat, si $i \leq l$, (p_i, q_i) est solution de Pell-Fermat. si $l|i$ donc dans ce cas, on a :

$$p_{i-1} + \sqrt{d}q_{i-1} > p_{l-1} + \sqrt{d}q_{l_1}$$

donc (p_{l-1}, q_{l-1}) est solution fondamentale.

3) Si l impaire, on a vu que (p_{2l-1}, q_{2l-1}) est une solution de (E), $x^2 - dy^2 = 1$. Si (p_{k-1}, q_{k-1}) est solution de Pell-Fermat alors $2l|k$ d'après la **Proposition 1.2.7.**

□

Chapitre 2

Approximation d'un nombre réel par des rationnels

2.1 Approximation d'un nombre réel par des rationnels

Définition 2.1.1. Soit ν un nombre réel > 0. Soit α un nombre réel. On dit que α est approximable à l'ordre μ s'il existe une constante, ne dépendant que de α, notée $c(\alpha)$ tel que l'inéquation $|\alpha - \frac{p}{q}| < \frac{c(\alpha)}{q^\nu}$ admet une infinité de solutions rationnels $\frac{p}{q}$.

Remarque. 1) Si α est un nombre réel irrationnel et $\frac{p_n}{q_n}$ un convergent de α, on a : $|\alpha - \frac{p_n}{q_n}| < \frac{1}{q_n^2}$. Donc α est approximable à l'ordre 2.

2) Si α est approximable à l'ordre ν alors il est approximable à l'ordre ν' pour tout $\nu' \leq \nu$.

3) Soit $\alpha \in \mathbb{R}$, on note $(\alpha) = \alpha - E(\alpha)$ alors α est approximable à l'ordre $\nu \Leftrightarrow (\alpha)$ est approximable à l'ordre ν.

$$\alpha - \frac{p}{q} = (\alpha) - \frac{p + qE(\alpha)}{q}$$

Theorème 2.1.1. *Un nombre rationnel est approximable à l'ordre 1 exactement (c'est-à-dire pas à un ordre supérieur à 1).*

Démonstration. Soit $\frac{a}{b} \in \mathbb{Q}$, $\text{PGCD}(a, b) = 1$, $b > 0$. Alors, il existe une infinité d'entiers, $p, q > 0$, $\text{PGCD}(p, q) = 1$ tel que $aq - bp = \pm 1$. Donc : $|\frac{a}{b} - \frac{p}{q}| < \frac{1}{bq}$ donc $\frac{a}{b}$ est approximable à l'ordre 1. Il faut remarquer que $|\frac{a}{b} - \frac{p}{q}| = \frac{|aq-bp|}{bq} > \frac{1}{bq}$. Soit $\nu > 1$, soit c une constante possitive ne dépendant que a et b. On doit montrer que l'inéquation $|\frac{a}{b} - \frac{p}{q}| < \frac{c}{q^\nu}$ n'admet qu'un nombre fini de solutions $\frac{p}{q}$. Soit $\frac{p}{q}$ un nombre rationnel tel que $|\frac{a}{b} - \frac{p}{q}| < \frac{c}{q^\nu}$. On a :

$$\frac{aq - bp}{bq} = \frac{a}{b} - \frac{p}{q}$$

Comme $aq - bp \neq 0$. On a : $|\frac{a}{b} - \frac{p}{q}| \geq \frac{1}{bq}$, d'où $\frac{1}{bq} < \frac{c}{q^\nu}$ donc $q^{\nu-1} < cb$. Donc $q < (cb)^{\frac{1}{\nu-1}}$. Or :

$$\left|\left|\frac{a}{b}\right| - \left|\frac{p}{q}\right|\right| < \left|\frac{a}{b} - \frac{p}{q}\right| < \frac{c}{q^\nu}$$

donc $|p| < \left(\frac{a}{b} + c\right)|q| < \left(|\frac{a}{b}| + c\right)(cb)^{\frac{1}{\nu-1}}$ donc il n'y a qu'un nombre fini de $\frac{p}{q}$ tel que :

$$\left|\frac{a}{b} - \frac{p}{q}\right| < \frac{c}{q^\nu}$$

□

Corollaire (Critère d'irrationnalité)**.** *Soit α un nombre réel, soient ν un nombre réel > 1 et $c > 0$. S'il existe une infinité d'irrationnels $\frac{p}{q}$ tel que $|\alpha - \frac{p}{q}| < \frac{c}{q^\nu}$ alors $\alpha \notin \mathbb{Q}$.*

Démonstration. Si les hypothèse du **Corrolaire** sont vérifiés, α est approximable à l'ordre ν avec $\nu > 1$, donc $\alpha \notin \mathbb{Q}$. □

Application 2.1.1.

$$\alpha = \sum_{n\geq 0}^{\infty} \frac{1}{2^{n!}} = \lim_{N\to+\infty} \sum_{n=0}^{N} \frac{1}{2^{n!}}$$

Cette limite existe. En effet, posons $u_N = \sum_{n=0}^{N} \frac{1}{2^{n!}}$, (u_N) est une suite croissante. On peut montrer que α est approximable à l'ordre 2.

Theorème 2.1.2 (Dirichlet)**.** *Tout nombre réel irrationnel est approximable à l'ordre 2.*

Démonstration du ***Théorème 2.1.2.***

Lemme 2.1.3 (Dirichlet)**.** *Soit β un nombre réel irrationnel. Soit Q un entier ≥ 1. Il existe au moins un nombre irrationnel $\frac{p}{q}$ tel que $q \leq Q$ et $|\beta - \frac{p}{q}| < \frac{1}{qQ}$.*

Démonstration du Lemme 2.1.3.

Notation. pour $x \in \mathbb{R}$, $(x) = x - E(x)$, $0 \leq (x) < 1$.

On considère les nombres 0, (β), (2β),...,$(Q\beta)$. Ces nombres sont deux à deux distincts, en effet, s'ils étaient distincts, il existerait k, k', $0 \leq k \leq Q$, $0 \leq k' \leq Q$, $k \neq k'$ tel que $(k\beta) = (k'\beta)$ donc $k\beta - E(k\beta) = k'\beta - E(k'\beta) \Rightarrow (k-k')\beta = E(k\beta) = E(k'\beta)$:

$$\Rightarrow \beta = \frac{E(k\beta) - E(k'\beta)}{k - k'} \in \mathbb{Q}$$

or $\beta \in \mathbb{Q}$. On a :

$$[0,1[= \left[0, \frac{1}{Q}\right[\cup \left[\frac{1}{Q}, \frac{2}{Q}\right[\cup ... \cup \left[\frac{Q-1}{Q}, 1\right[= \bigcup_{k=1}^{Q} \left[\frac{k-1}{Q}, \frac{k}{Q}\right[$$

Les $(Q+1)$ nombres 0, (β), ..., $(Q\beta)$ appartiennent à la réunion disjointe de Q intervalles $[0, \frac{1}{Q}[\cup ... \cup [\frac{Q-1}{Q}, 1[$ parmi les nombres 0, (β), ..., $(Q\beta)$ appartiennent au même intervalle.

Donc il existe k, k', $0 \leq k < Q$, $0 \leq k' < Q$, $k > k'$ tel que $|(k\beta) - (k'\beta)| < \frac{1}{Q}$.

$$\Rightarrow \left|\beta - \frac{E(k\beta) - E(k'\beta)}{k - k'}\right| < \frac{1}{(k-k')Q}$$

On pose : $p = E(k\beta) - E(k'\beta)$ et $q = k - k'$. On a bien $|\beta - \frac{p}{q}| < \frac{1}{qQ}$. □ □

Grâce au *Lemme 2.1.3.*, nous pouvons démontrer par l'absurde le **Théorème 2.1.2.**. Supposons qu'il existe un nombre fini de rationnels

$$\frac{p_1}{q_1}, ..., \frac{p_m}{q_m} \text{ tel que } \left|\beta - \frac{p_i}{q_i}\right| < \frac{1}{q_i^2},\ i = \{1, ..., m\}$$

On pose :

$$Q = \left[\frac{1}{\min\limits_{1\leq i\leq m} \left|\beta - \frac{p_i}{q_i}\right|}\right] + 1 \geq 1$$

D'après le **Lemme 2.1.3.**, il existe un rationnel $\frac{p}{q}$ tel que $q \leq Q$ et

$$\left|\beta - \frac{p}{q}\right| < \frac{1}{qQ} < \min_{1\leq i\leq m}\left|\beta - \frac{p_i}{q_i}\right|$$

donc :

$$\frac{p}{q} \notin \left\{\frac{p_1}{q_1}, ..., \frac{p_m}{q_m}\right\}$$

Or $q \leq Q$ donc $\left|\beta - \frac{p}{q}\right| < \frac{1}{q^2}$. CONTRADICTION !

Donc : β est approximable à l'ordre 2. □

Theorème 2.1.4. *Soit α un nombre réel quadratique. Alors α n'est pas approximable à un ordre supérieur à 2.*

Démonstration. Soit α un nombre réel quadratique. α admet un développement en fractions continues périodique.

$$\alpha = [a_0, ..., a_k, \overline{a_{k+1}, ..., a_n}]$$

Soit M un majorant de $(a_0, a_1, ..., a_n)$. Soit $\frac{p_n}{q_n}$ un convergent de α. On a $q_n = a_n q_{n-1} + q_{n-2}$, $n \geq 2$. Donc : $q_n \leq (M+1)q_{n-1}$, $n \geq 1$. Soit $\alpha_m = [a_m, a_{m+1}, ...]$ ($m$ième quotient complet de α). On a $\alpha_m \leq \alpha_m + 1 \leq M + 1$. Soit $\frac{p}{q}$ un rationnel, $q > 0$, PGCD$(p, q) = 1$. Soit n' le plus grand entier tel que $q_{n'} \leq q$. Donc on a : $q_{n'} \leq q < q_{n'+1}$. D'après le **Théorème 1.1.6.** (Théorème de Lagrange), on a : $|\alpha - \frac{p}{q}| \geq |\alpha - \frac{p_{m'+1}}{q_{m'+1}}|$. Or :

$$\alpha = \frac{p_{n'+1}\alpha_{n'+2} + p_{n'}}{q_{n'+1}\alpha_{n'+2} + q_{n'}}$$

Donc :

$$\begin{aligned}\left|\alpha - \frac{p_{n'+1}}{q_{n'+1}}\right| &= \left|\frac{p_{n'+1}\alpha_{n'+2} + p_{n'}}{q_{n'+1}\alpha_{n'+2} + q_{n'}} - \frac{p_{n'+1}}{q_{n'+1}}\right| \\ &= \left|\frac{p_{n'}q_{n'+1} - q_{n'}p_{n'+1}}{q_{n'+1}\alpha_{n'+2} + q_{n'}q_{n'+1}}\right| \\ &= \left|\frac{1}{q_{n'+1}\alpha_{n'+2} + q_{n'} + q_{n'+1}}\right|\end{aligned}$$

Donc : $|\alpha - \frac{p_{n'+1}}{q_{n'+1}}| \leq \frac{1}{2(M+1)^3 q_{n'}^2}$. On pose $c = \frac{1}{2(M+1)^3}$. On a :

$$\left|\alpha - \frac{p_{n'+1}}{q_{n'+1}}\right| \leq \frac{c}{q_n^2} \leq \frac{c}{q^2}$$

car $q_{n'} \leq q$. D'où $|\alpha - \frac{p}{q}| \leq \frac{c}{q^2}$.

Soit ν un nombre supérieure à 2. Soit $\frac{p}{q}$ un nombre rationnel tel que $|\alpha - \frac{p}{q}| < \frac{1}{q^\nu}$ donc :

$$\frac{c}{q^2} < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\nu}$$

donc $q^{\nu-2} < \frac{1}{c}$ donc : $q < \frac{1}{c^{\frac{1}{\nu-2}}}$. Or $\left||\frac{p}{q}| - |\alpha|\right| \leq |\frac{p}{q} - \alpha| < 1 \Rightarrow |\frac{p}{q}| < |\alpha| + 1$. Donc $|p| < (\alpha+1)q < \frac{(\alpha+1)}{c^{\frac{1}{\nu+2}}}$. Donc : il n'y a qu'un nombre fini de rationnels $\frac{p}{q}$ tels que $|\alpha - \frac{p}{q}| < \frac{1}{q^\nu}$. α n'est pas approximable à l'ordre ν si $\nu > 2$. □

Application 2.1.2 (Suite de l'**Application 2.1.1.**). Rappelons que

$$\alpha = \sum_{n=0}^{\infty} \frac{1}{2^{n!}}$$

On montre que α est approximable à l'orde 2.

$$\sum_{n=0}^{\infty} \frac{1}{2^{n!}} = \frac{p_N}{q_N} \text{ avec } q_N = 2^{N!}$$

$$\left|\alpha - \frac{p_N}{q_N}\right| < \frac{c}{q_N^2}$$

Or :

$$\begin{aligned} \alpha - \frac{p_N}{q_N} = \sum_{n=N+1}^{\infty} \frac{1}{2!} &= \frac{1}{2^{N+1!}} + \frac{1}{2^{N+2!}} + ... \\ &= \frac{1}{2^{N+1!}} \left(1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{6} + ...\right) \\ &= \frac{1}{2^{N+1!}} \sum \frac{1}{2^n} \leq \frac{1 \times 2}{2^{(N+1)!}} \leq \frac{2}{2^{2N!}} \leq \frac{2}{q_N^2} \end{aligned}$$

Avec le même type de raisonnement, on montre que α est approximable à un ordre ν quelconque.

$$\left|\alpha - \frac{p_N}{q_N}\right| < \frac{c}{q^\nu} \qquad \alpha - \frac{p_N}{q_N} = \sum_{n=N+1}^{\infty} \frac{1}{2^{n!}}$$

$$\sum_{n=N+1}^{\infty} = \frac{1}{2^{N+1!}} + \frac{1}{2^{N+2!}} + ... \leq \frac{1}{2^{N+1!}} \left(\sum \frac{1}{2^n}\right) \qquad (*)$$

Or $\sum \frac{1}{2^n} = 2$. Donc : $(*) \leq \frac{2}{2^{N+1!}}$. Pour ν fixé, $\forall N > \nu$, on a : $N + 1 \geq \nu N!$. Donc :

$$(*) \leq \frac{2}{2^{N+1!}} \leq \frac{2}{2^{\nu N!}} \leq \frac{2}{q_N^2}$$

Définition 2.1.2. On dit que α est algébrique s'il existe un polynôme $P(X)$ non nul à coefficient dans $\mathbb{Q}$ tel que $P(\alpha) = 0$, c'est-à-dire il existe $a_0, a_1, ..., a_n \in \mathbb{Q}$ non tous nuls tel que

$$a_0 + a_1\alpha + ... + a_n\alpha^n = 0$$

Exemple 2.1.1.
- nombres quadratiques
- $\sqrt[3]{2}$ est algébrique car $\sqrt[3]{2}$ est racine de $X^3 - 2$
- $\sqrt[n]{k}$ est algébrique car il est racine de $X^n - k$.
- $\imath$ est algbérique car il est racine de $X^2 + 1$
- $\jmath = \exp\left(\frac{2\imath\pi}{3}\right)$ racine de $X^2 + X + 1$ donc algébrique
- e, π ne sont pas algébriques (ils sont transcendent).

Définition 2.1.3. Soit α un nombre algébrique. Parmi les polynômes non nuls à coefficients dans $\mathbb{Q}$ annulant α, il en existe un de degré minimal et unitaire ($a_n = 1$). On appelle degré de α sur $\mathbb{Q}$ le degré de ce polynôme. On le note $\deg \alpha$.

Exemple 2.1.2.
- $\deg \sqrt[3]{2} = 3$
- $\deg \imath = 2$
- $\deg \jmath = 2$
- si $a \in \mathbb{Q}$ racine de $X - a$ alors $\deg a = 1$.

Theorème 2.1.5 (Théorème de Liouville)**.** *Soit α un nombre algébrique de degré $d > 1$ alors il existe un réel $c > 0$ ne dépendant que de α tel que pour tout rationnel $\frac{p}{q}$, $\text{PGCD}(p, q) = 1$, $q > 1$, on ait :*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^d}$$

Démonstration. Soit α un nombre algébrique de degré $d > 1$. Soit $\frac{p}{q} \in \mathbb{Q}$, si $|\alpha - \frac{p}{q}| > 1$, on a $\left(\alpha - \frac{p}{q}\right) > \frac{1}{q^d}$. Si $\left|\alpha - \frac{p}{q}\right| \leq 1$, soit $P(X)$ le polynôme de $\mathbb{Q}[X]$ de degré d tel que $P(\alpha) = 0$. On a :

$$P\left(\frac{p}{q}\right) = P\left(\frac{p}{q}\right) - P(\alpha)$$

D'après le théorème des accroissements finies, on a :

$$\left|P\left(\frac{p}{q}\right) - P(\alpha)\right| \leq \left|\frac{p}{q} - \alpha\right| \times \max_{\frac{p}{q} < \theta < \alpha} |P'(\theta)| \leq \left|\frac{p}{q} - \alpha\right| \times \max_{\theta \in [\alpha-1, \alpha+1]} |P'(\theta)| \qquad (*)$$

On pose $c' = \max\limits_{\theta \in [\alpha-1, \alpha+1]} |P'(\theta)|$. $(*)$ devient :

$$\frac{1}{c'}\left|P\left(\frac{p}{q}\right) - P(\alpha)\right| \leq \left|\frac{p}{q} - \alpha\right|$$

On pose aussi :

$$P(X) = a_0 + a_1 X + ... + a_d X^d,\ a_i \in \mathbb{Q},\ a_d \neq 0$$

On a :

$$P\left(\frac{p}{q}\right) - P(\alpha) = P\left(\frac{p}{q}\right) = a_0 + a_1\frac{p}{q} + ... + a_d\left(\frac{p}{q}\right)^d$$

$$= \frac{a_0 q^d + a_1 p q^{d-1} + a_2 p^2 q^{d-2} + ... + a_d p^d}{q^d}$$

Or : $P\left(\frac{p}{q}\right) \neq 0$ donc $a_0 q^d + a_1 p q^{d-1} + a_2 p^2 q^{d-2} + ... + a_d p^d$ est un entier non nul. Donc :

$$\left|P\left(\frac{p}{q}\right) - P(\alpha)\right| > \frac{1}{q^d}$$

d'où $|\frac{p}{q} - \alpha| \geq \frac{1}{c' q^d}$. On pose $c = \frac{1}{c'}$, on a : $|\frac{p}{q} - \alpha| > \frac{c}{q^d}$. □

Corollaire. *Soit α un nombre algébrique de degré $d > 1$. Alors α n'est pas approximable à l'ordre $\nu > d$.*

Démonstration. Soit c'' un nombre réel > 0 et ν un nombre réel $> d$. On montre que le nombre de rationnels $\frac{p}{q}$ tels que :

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{c''}{q^\nu}$$

est fini. Soit $\frac{p}{q}$ un rationnel tel que :

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{c''}{q^\nu} \qquad (*)$$

D'après le **Théorème 2.1.5.**, on a $|\alpha - \frac{p}{q}| \geq \frac{c}{q^d}$. donc :

$$\frac{c}{q^d} < \frac{c''}{q^\nu}$$

D'où $q^{\nu-d} \leq \frac{c''}{c}$. Donc :

$$q \leq \left(\frac{c''}{c}\right)^{\frac{1}{\nu-d}}$$

Or $|\alpha - \frac{p}{q}| \leq \frac{c''}{q^d}$ donc $|\frac{p}{q} - \alpha| \leq \frac{c''}{q^\nu}$ d'où :

$$\left|\frac{p}{q}\right| \leq \alpha + \frac{c''}{q^\nu} < |\alpha| + c''$$

Donc :

$$|p| < q(|\alpha| + c'') \leq \left(\frac{c''}{c}\right)^{\frac{1}{\nu-d}} (|\alpha| + c'')$$

Donc si $\frac{p}{q}$ vérifie $(*)$ alors $q \leq \left(\frac{c''}{c}\right)^{\frac{1}{\nu-d}}$ et $|p| \leq \left(\frac{c''}{c}^{\frac{1}{\nu-d}}\right) (|\alpha| + c'')$. Donc il n'y a qu'un nombre finis de rationnels $\frac{p}{q}$ tels que $|\alpha - \frac{p}{q}| \leq \frac{c''}{q^\nu}$ pour $\nu > d$. □

Application 2.1.3 (Suite de l'**Application 2.1.2.**)**.**

$$\alpha = \sum_{n=0}^{\infty} \frac{1}{2^{n!}}$$

α est approximable à tout ordre. D'après le **Corrolaire**, α n'est pas algébrique.

Chapitre 3

Corps quadratiques

3.1 Corps quadratiques

Soit D un entier (positif ou négatif) non carré.

Notation. si $D < 0$, on pose $\sqrt{D} = i\sqrt{|D|}$, on note $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D},\ a \in \mathbb{Q},\ b \in \mathbb{Q}\}$.

Remarque. si $a + b\sqrt{D} = a' + b'\sqrt{D}$, $a, b, a', b' \in \mathbb{Q}$ alors $(a - a') = (b - b')\sqrt{D}$. Si $b \neq b'$, on a $\sqrt{D} = \frac{a-a'}{b-b'} \in \mathbb{Q}$ absurde car D n'est pas carré. Donc $a = a'$ et $b = b'$.

Theorème 3.1.1. *$\mathbb{Q}(\sqrt{D})$ est un sous-corps de $\mathbb{C}$ contenant $\mathbb{Q}$.*

Démonstration.
- $\mathbb{Q} \subset \mathbb{Q}(\sqrt{D})$
- $a, b, a', b' \in \mathbb{Q}$

$$(a + b\sqrt{D}) - (a' + b'\sqrt{D}) = a - a' + (b - b')\sqrt{D} \in \mathbb{Q}(\sqrt{D})$$

  donc $\mathbb{Q}(\sqrt{D})$ stable par addition.
- $(a + b\sqrt{D})(a' + b'\sqrt{D}) = aa' + bb'D + (ab' + ba')\sqrt{D} \in \mathbb{Q}(\sqrt{D})$. Donc : $\mathbb{Q}(\sqrt{D})$ est stable par multiplication.

– Soit $\alpha \in \mathbb{Q}(\sqrt{D})\backslash\{0\}$, $x = a + b\sqrt{D}$ avec $(a, b) \neq (0, 0)$.

$$\frac{1}{x} = \frac{1}{a + b\sqrt{D}} = \frac{a - b\sqrt{D}}{a^2 - b^2D} = \frac{a}{a^2 - b^2D} - \frac{b}{a^2 - b^2D}\sqrt{D} \in \mathbb{Q}(\sqrt{D})$$

Donc : $(\mathbb{Q}(\sqrt{D}), +, \times)$ est un corps. □

Theorème 3.1.2. *$(\mathbb{Q}(\sqrt{D}), +, \times)$ est un espace vectoriel sur $\mathbb{Q}$ et $\{1, \sqrt{D}\}$ est une base de $\mathbb{Q}(\sqrt{D})$ sur $\mathbb{Q}$.*

Démonstration. $\mathbb{Q}$ est un sous-corps de $\mathbb{Q}(\sqrt{D})$ donc $(\mathbb{Q}(\sqrt{D}, +, \times)$ est un espace vectoriel sur $\mathbb{Q}$.

$\forall x \in \mathbb{Q}$, $\exists!(a, b) \in \mathbb{Q}^2$ tel que $x = a + b\sqrt{D}$ donc $\{1, \sqrt{D}\}$ est une base de $\mathbb{Q}(\sqrt{D})$ sur $\mathbb{Q}$. Donc :

$$\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{D})) = 2$$

□

Rappel. si $D < 0$, $\sqrt{D} = i\sqrt{|D|}$.

Proposition 3.1.3. *Soit $\alpha \in \mathbb{Q}(\sqrt{D})$ alors ou bien $\alpha \in \mathbb{Q}$ ou α est quadratique.*

Démonstration. Soit $\alpha \in \mathbb{Q}(\sqrt{D})$, $\alpha = a + b\sqrt{D}$, $a, b \in \mathbb{Q}$. Si $\alpha \notin \mathbb{Q}$, on a $b \neq 0$.

$$\alpha - a = b\sqrt{D} \Leftrightarrow (\alpha - a)^2 = b^2 D$$

d'où :

$$\alpha^2 - 2a\alpha + \alpha^2 - b^2 D = 0$$

Donc α est racine de :

$$X^2 - \underbrace{2a}_{\mathbb{Q}} X + \underbrace{a^2 - b^2 D}_{\mathbb{Q}} = 0$$

Donc : α est quadratique. □

Notation. Soit $\alpha \in \mathbb{Q}(\sqrt{D})$, $\alpha = a + b\sqrt{D}$. On note $\overline{\alpha} = a - b\sqrt{D}$.

$$\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha} \qquad (\text{Trace de } \alpha)$$

$$N(\alpha) = \alpha\overline{\alpha} \qquad (\text{Norme de } \alpha)$$

Proposition 3.1.4. *Soit $\alpha \in \mathbb{Q}(\sqrt{D})$ alors :*

$$\begin{cases} \mathrm{Tr}(\alpha) \in \mathbb{Q} \\ N(\alpha) \in \mathbb{Q} \end{cases}$$

Démonstration. Soit $\alpha = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ et $\overline{\alpha} = a - b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$.

$$\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha} = 2a$$

$$N(\alpha) = \alpha\overline{\alpha} = a^2 - b^2 D$$

Donc : $\mathrm{Tr}(\alpha) \in \mathbb{Q}$ et $N(\alpha) \in \mathbb{Q}$. □

Remarque. Si $D < 0$, $N(\alpha) \in \mathbb{Q}^+$.

3.2 Entiers de $\mathbb{Q}(\sqrt{D})$

Définition 3.2.1. Soit $\alpha \in \mathbb{Q}(\sqrt{D})$ on dit que α est un entier de $\mathbb{Q}(\sqrt{D})$ si et seulement si $\mathrm{Tr}(\alpha) \in \mathbb{Z}$ et $N(\alpha) \in \mathbb{Z}$.

Proposition 3.2.1. *Soit $\alpha \in \mathbb{Q}(\sqrt{D})$, α est un entier de $\mathbb{Q}(\sqrt{D})$ si et seulement si α est racine d'une équation de la forme $X^2 + cX + d = 0$ avec $c, d \in \mathbb{Q}$.*

Démonstration. ($\Rightarrow$) Soit α un entier de $\mathbb{Q}(\sqrt{D})$ donc $\alpha = a + b\sqrt{D}$, on a :

$$\begin{cases} \mathrm{Tr}(\alpha) = 2a \in \mathbb{Z} \\ N(\alpha) = a^2 - b^2 D \in \mathbb{Z} \end{cases}$$

Or α est racine de $X^2 - \underbrace{2a}_{\mathbb{Q}} X + \underbrace{a^2 - b^2 D}_{\mathbb{Q}}$.

($\Leftarrow$) Soit $\alpha \in \mathbb{Q}(\sqrt{D})$, supposons que α est racine d'une équation de la forme :

$$X^2 + cX + d = 0 \qquad c, d \in \mathbb{Z}$$

$\alpha = a + b\sqrt{D}$. On vérifie que $\overline{\alpha} = a - b\sqrt{D}$ est racine de $X^2 + cX + d = 0$. Donc :

$$X^2 + cX + d = (X - \alpha)(X - \overline{\alpha})$$

$\Rightarrow c = -(\alpha + \overline{\alpha}) = -\mathrm{Tr}(\alpha)$ et $d = \alpha \times \overline{\alpha} = N(\alpha)$. Donc : $\mathrm{Tr}(\alpha) \in \mathbb{Z}$ et $N(\alpha) \in \mathbb{Z}$.

□

Notation. $K = \mathbb{Q}(\sqrt{D})$, on note : $\mathbb{Z}_K$ l'ensemble des entiers de K.

Proposition 3.2.2. *Soit D entier sans facteur carré et $\alpha \in \mathbb{Z}_{\mathbb{Q}(\sqrt{D})}$ ($\alpha = a + b\sqrt{D}$). Si $D \equiv 2[4]$ ou $D \equiv 3[4]$ alors $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. Si $D \equiv 1[4]$ alors $a = \frac{a'}{2}$ et $b = \frac{b'}{2}$ avec a' et b' entiers de même parité.*

Démonstration. Soit $\alpha = a + b\sqrt{D}$ un entier de $\mathbb{Q}(\sqrt{D})$. On pose

$$a = \frac{a_1}{a_2} \qquad \mathrm{PGCD}(a_1, a_2) = 1$$

$$b = \frac{b_1}{b_2} \qquad \mathrm{PGCD}(b_1, b_2) = 1$$

$\mathrm{Tr}(\alpha) = 2a = 2\frac{a_1}{a_2} \in \mathbb{Z}$. Donc $a_2 | 2a_1$ et comme $\mathrm{PGCD}(a_1, a_2) = 1$ alors $a_2 | 2$. Donc $a_2 = 1$ ou $a_2 = 2$.

1) Si $a_2 = 1$, $N(\alpha) = a^2 - b^2 D \in \mathbb{Z} \Rightarrow a_1^2 - \frac{b_1^2}{b_2^2} D \in \mathbb{Z} \Rightarrow \frac{b_1^2}{b_2^2} D \in \mathbb{Z}$. Donc : $b_2^2 | b_1^2 D$ et comme $\mathrm{PGCD}(b_2, b_1) = 1$ alors $b_2^2 | D$. Or D est sans facteur carré donc $b_2 = 1$. Dans ce cas, $a, b \in \mathbb{Z}$.
2) Si $a_2 = 2$, $N(\alpha) = \frac{a_1^2}{4} - \frac{b_1^2}{b_2^2} D \in \mathbb{Z}$ donc

$$\frac{b_2^2 a_1^2 - 4 b_1^2 D}{4 b_2^2} \in \mathbb{Z}$$

Donc : $4 | b_2^2 a_1^2 - 4 b_1^2 D \Rightarrow 4 | b_2^2 a_1^2$. Or $\mathrm{PGCD}(a_1, a_2) = (a_1, 2) = 1$. Donc $b_2 = 2b_2'$. Donc $N(\alpha) = \frac{a_1^2}{4} - \frac{b_1^2 D}{4 b_2^2} \in \mathbb{Z}$ d'où $a_1^2 - \frac{b_1^2 D}{b_2'} \in \mathbb{Z}$. Donc $\frac{b_1^2 D}{b_2'} \in \mathbb{Z}$. D'où $b_2'^2 | b_1^2 D$. Or $\mathrm{PGCD}(b_1, b_2) = 1$ donc $b_2'^2 | D$ or D est sans facteur carré donc $b_2' = 1$. Dans ce cas, on a : $a = \frac{a_1}{2}$ et $b = \frac{b_1}{2}$ (avec $a_1 \not| 2$ et $b_1 \not| 2$). or $\frac{a_1^2 - b_1^2 D}{4} \in \mathbb{Z}$ donc $a_1^2 - b_1^2 D \equiv 0[4]$, comme $a_1 \equiv 1[2]$ et $b_1 \equiv 1[2] \Rightarrow a_1^2 \equiv 1[4]$ et $b_1^2 \equiv 1[4]$ donc : $1 - D \equiv 0[4]$ donc $D \equiv 1[4]$.

□

Corollaire. *Soit $K = \mathbb{Q}(\sqrt{D})$. Si $D = 2$ ou $3[4]$:*

$$\mathbb{Z}_K = \{a + b\sqrt{D},\ a, b \in \mathbb{Z}\}$$

Si $D \equiv 1[4]$:

$$\mathbb{Z}_K = \{\frac{a + b\sqrt{D}}{2},\ a, b \text{ entiers de même partié}\}$$

$(\mathbb{Z}_K, +, \times)$ est un sous-anneau de K.

Démonstration. Il suffit de montrer que $\mathbb{Z}_K$ est stable par multiplication et par addition. □

3.3 Eléments inversibles dans $\mathbb{Z}_K$

Définition 3.3.1. Soit $\alpha \in \mathbb{Z}_K$. On dit que α est inversible dans $\mathbb{Z}_K$ si et seulement si il existe α' dans $\mathbb{Z}$ tel que $\alpha \times \alpha' = 1$.

Proposition 3.3.1. *Soit α un élément de $\mathbb{Z}_K$. α est inversible dans $\mathbb{Z}_K \Leftrightarrow N(\alpha) = 1$ ou -1.*

Démonstration. ($\Rightarrow$) Soit α un élément inversible de $\mathbb{Z}_K$ alors il existe α' dans $\mathbb{Z}_K$ tel que $\alpha \in \alpha' = 1$. Or $N(\alpha \times \alpha') = N(\alpha) \times N(\alpha')$. Donc : $\underbrace{N(\alpha)}_{\in\mathbb{Z}} \times N(\alpha') = 1$, donc $N(\alpha) = 1$ ou $N(\alpha) = -1$.

($\Leftarrow$) Soit $\alpha \in \mathbb{Z}_K$ tel que $N(\alpha) = 1$ ou -1 on a :

$$\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha} \in \mathbb{Z}$$

$$N(\alpha) = \alpha\overline{\alpha} \in \mathbb{Z}$$

Cela entraine que $\overline{\alpha} \in \mathbb{Z}_K$. Or $N(\alpha) = 1$ ou $-1 \Rightarrow \alpha\overline{\alpha} = 1$ ou -1, donc α est inversible dans $\mathbb{Z}_K$ et son inverse est : $\overline{\alpha}$ si $N(\alpha) = 1$ ou $-\overline{\alpha}$ si $N(\alpha) = -1$.

□

Remarque.

- Si $D < 0$ $\alpha = a + b\sqrt{D}$ est inversible dans $\mathbb{Z}_{\mathbb{Q}(\sqrt{D})}$ si et seulement si $N(\alpha) = a^2 - b^2D = 1$.
  - ∗ Si $D = -1$, $K = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$

$$\mathbb{Z}_K = \{a + bi,\ a, b \in \mathbb{Z}\}$$

$a^2 + b^2 = 1 \Leftrightarrow a = \pm 1 b = 0$ ou $a = 0, b = \pm 1$. Les éléments inversibles dans $\mathbb{Q}(i)$ sont :

$$\{1, -1, i, -i\}$$

  - ∗ Si $D < -1$, $D \equiv 2$ ou $3[4]$, $\alpha = a + b\sqrt{D}$ est inversible dans $\mathbb{Z}_{\mathbb{Q}(\sqrt{D})} \Leftrightarrow a^2 - b^2D = 1$, $a, b \in \mathbb{Z} \Leftrightarrow b = 0$ et $a = \pm 1$. Les seuls élement inversibles sont $\{1, -1\}$.
  - ∗ Si $D < -1$ et $D \equiv 1[4]$, $\alpha = a + b\sqrt{D}$ est inversible dans $\mathbb{Z}_{\mathbb{Q}(\sqrt{D})} \Leftrightarrow a^2 - b^2D = 1$. Si $a \in \mathbb{Z}$ alors $b \in \mathbb{Z}$, $a^2 - b^2D = 1 \Rightarrow a = 1$ ou $a = -1$ et $b = 0$.
    Si $a \in \mathbb{Z}$, $a = \frac{a'}{2}$ et $b = \frac{b'}{2}$ (avec a' et b' impaire), $a^2 - b^2D \Leftrightarrow a'^2 - b'^2D = 4$. Or $-D = 3[4]$ donc $a' = \pm 2$ et $b' = 0$. Or a' est impaire. Donc les éléments inversibles de $\mathbb{Z}_{\mathbb{Q}(\sqrt{D})}$ sont $\{1, -1\}$.
- si $D > 0$, l'équation de Pell-Fermat $x^2 - y^2D = 1$ admet une infinité de solutions donc il y a un nombre infini d'éléments inversibles dans $\mathbb{Z}_{\mathbb{Q}(\sqrt{D})}$.

3.4 Arithmétique dans $\mathbb{Z}_K$

Soit D un entier sans facteur carré. Soit $K = \mathbb{Q}(\sqrt{D})$, "corps quadratique" (avec la notation $\sqrt{D} = i\sqrt{|D|}$ si $D < 0$). Soit $\mathbb{Z}_K$ l'anneau des entiers de K.

3.4.1 Divisibilité dans $\mathbb{Z}_K$

Définition 3.4.1. Soient $x, y \in \mathbb{Z}_K$, on dit que x divise y et on note $y|x$ s'il existe $z \in \mathbb{Z}_K$ tel que $y = xz$.

Propriété 3.4.1. *1)* $\forall x \in \mathbb{Z}_K$, $x|x$

2) $\forall x \in \mathbb{Z}_K$, $\forall y \in \mathbb{Z}_K$, $x|y$ *et* $y|x \Leftrightarrow \exists u$ *inversible dans* $\mathbb{Z}_K$ *tel que* $x = uy$.

3) $\forall x \in \mathbb{Z}_K$, $\forall y \in \mathbb{Z}_K$, $\forall z \in \mathbb{Z}_K$, $x|y$ *et* $y|z \Leftrightarrow x|z$.

Démonstration. 1) $x = 1x$ donc $x|x$.

2) ($\Rightarrow$) si $x|y$ et $y|x$ alors il existe $z \in \mathbb{Z}_K$ tel que $y = zx$ et $x = z'y$ donc $x = zz'x$. Donc : $x(1 - z'z) = 0$.
- Si $x = 0$, on a $y = 0$.
- Si $x \neq 0$, on a $zz' = 1$.

Donc z est inversible dans $\mathbb{Z}_K$ d'inverse z'.

($\Leftarrow$) si $x = uy$ avec u inversible dans $\mathbb{Z}_K$. Si u' est l'inverse de u, on a $u'x = y$ donc $y|x$ et $x|y$.

3) évident

□

Remarque. Les éléments inversibles de $\mathbb{Z}_K$ jouent le rôle de $\{1, -1\}$ dans $\mathbb{Z}$.

Notation. On note $U(\mathbb{Z}_K)$ l'ensemble des éléments inversibles (unités) de $\mathbb{Z}_K$.

Remarque. 1) $u \in U(\mathbb{Z}_K) \Leftrightarrow N(u) = 1$ ou -1. Si $u = a + b\sqrt{d}$.

$$N(u) = a^2 - b^2 D$$

2) $\forall x \in \mathbb{Z}_K$, $\forall u \in U(\mathbb{Z}_K)$, on a $u|x$.

Démonstration. $u \in U(\mathbb{Z}_K)$ s'il existe $u' \in \mathbb{Z}_K$ tel que $uu' = 1$ donc $x = u\underbrace{u'x}_{\in \mathbb{Z}_K}$ donc $u|x$ pour tout $x \in \mathbb{Z}_K$. □

3.4.2 Elements irréductibles dans $\mathbb{Z}_K$

Définition 3.4.2. Soit $x \in \mathbb{Z}_K$, on dit que x est irréductible dans $\mathbb{Z}_K$ si et seulement si les seuls divisieurs de x sont les éléments de $U(\mathbb{Z})$ ou les éléments de la forme ux ($u \in U(\mathbb{Z})$).

Définition 3.4.3. Les éléments de la forme ux avec $u \in U(\mathbb{Z}_K)$ sont appelés les éléments associés à x.

Proposition 3.4.2. *Soit* $x \in \mathbb{Z}_K$ *tel que* $|N(x)|$ *est un nombre premier de* $\mathbb{Z}$. *Alors* x *est irréductible dans* $\mathbb{Z}_K$.

Démonstration. Soit $x \in \mathbb{Z}_K$ tel que $|N(x)|$ est un nombre premier de $\mathbb{Z}$. Supposons que $x = y \times z$ dans $\mathbb{Z}_K$ donc $N(x) = N(yz) = N(y)N(z)$. Donc $|N(x)| = |N(y)||N(z)|$. Or $|N(x)|$ est un nombre premier donc $|N(y)| = 1$ ou $|N(z)| = 1$.
- Si $N(y) = 1$ alors $y \in U(\mathbb{Z}_K)$ (c'est-à-dire y est inversible dans $\mathbb{Z}_K$).
- Si $N(z) = 1$ alors $z \in U(\mathbb{Z}_K)$ (c'est-à-dire z est inversible dans $\mathbb{Z}_K$). $x = yz$ $y = xz'$ aec z' inverse de z.

Les seuls diviseurs de x sont les éléments inversibles ($U(\mathbb{Z}_K)$) ou de la forme ux (où $u \in \mathbb{Z}_K$). □

3.4.3 Eléments premiers entre eux

Définition 3.4.4. Soient $x, y \in \mathbb{Z}_K$, on dit que x et y sont premiers entre eux si et seulement si les seuls diviseurs communs à x et y sont les éléments inversibles de $\mathbb{Z}_K$ ($U(\mathbb{Z}_K)$).

Définition 3.4.5. On dit que $\mathbb{Z}_K$ est un anneau euclidien pour la norme si et seulement si $\forall x \in \mathbb{Z}_K$, $\forall y \in \mathbb{Z}_K\{0\}$, il existe q, r dans $\mathbb{Z}_K$ vérifiant $x = yq + r$ avec $r = 0$ ou $|N(r)| < N|(y)|$.

Si $\mathbb{Z}_K$ est un anneau euclidien pour la norme, alors $\mathbb{Z}_K$ possède une arithmétique analogue à celle de $\mathbb{Z}$. On peut définir l'analogue du PGCD.

3.4.4 PGCD dans $\mathbb{Z}_K$ quand $\mathbb{Z}_K$ est euclidien pour la norme

Définition 3.4.6. Soit $x, y \in \mathbb{Z}_K$

$$A_{x,y} = \{|N(z)|, z|x \text{ et } z|y \text{ avec } z \in \mathbb{Z}_K\}$$

$A_{x,y} \subset \mathbb{N}$ et est non vide. $\forall u \in U(\mathbb{Z}_K)$, u est un diviseur commun de x et et de y. Donc $N|(u)| = 1 \in A_{x,y}$.

$A_{x,y}$ admet un plus petit élément $|N(z_0)|$ où z_0 est un diviseur commun de x et y.

Un PGCD "à éléments inversibles près de x et de y" est z_0.

Theorème 3.4.3. *Si $\mathbb{Z}_K$ est euclidien pour la norme, on a le théorème fondamental pour l'arithmétique dans $\mathbb{Z}_K$ suivant :*

$\forall x \in \mathbb{Z}_K \backslash U(\mathbb{Z}_K)$ alors x se décompose en facteurs irréductibles dans $\mathbb{Z}_K$.

$$x = u \times p_1^{e_1} ... p_k^{e_k}$$

avec $u \in U(\mathbb{Z}_K)$, $p_1, ..., p_k$ irréductibles dans $\mathbb{Z}_K$ et $e_1, ..., e_k \in \mathbb{N}$. Cette décomposition est unique à l'ordre des facteurs près et à éléments inversibles près.

3.4.5 Exemples d'anneaux euclidiens

1) $\mathbb{Z}[i] = \{a + bi,\ a \in \mathbb{Z},\ b \in \mathbb{Z}\}$ anneau des entiers de $\mathbb{Q}(i)$.

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$$

Theorème 3.4.4. *$\mathbb{Z}[i]$ est euclidien pour la norme, c'est-à-dire $\forall x \in \mathbb{Z}[i]$, $\forall y \in \mathbb{Z}[i]\backslash\{0\}$, $\exists (q, r) \in \mathbb{Z}[i]^2$ tel que $x = yq + r$ avec $r = 0$ ou $N(r) < N(y)$.*

Démonstration. Soient $x \in \mathbb{Z}[i]$ et $y \in \mathbb{Z}[i]\backslash\{0\}$, $\frac{x}{y} \in \mathbb{Q}(i)$, $\frac{x}{y} = A + Bi$ avec $A \in \mathbb{Q}$ et $B \in \mathbb{Q}$.

Soit a l'entier "le plus proche" de A et b l'entier le plus proche de B, on a :

$$|A - a| \leq \frac{1}{2}$$

$a = E(A)$ ou $E(A) + 1$.

$$|B - b| \leq \frac{1}{2}$$

$$N((A + Bi) - (a + bi)) = N(A - a + (B - b)i) = (A - a)^2 + (B - b)^2 \leq \frac{1}{4} + \frac{1}{4} \leq \frac{1}{2}$$

□

2) Soit $j = e^{\frac{2i\pi}{3}}$:

$$\mathbb{Z}[j] = \{a + bj,\ a \in \mathbb{Z},\ b \in \mathbb{Z}\}$$

$$N(a + bj) = (a + bj)(a + b\bar{j}) = a^2 + b^2 j\bar{j} + ab(j + \bar{j}) = a^2 + b^2 - ab = \left(a - \frac{1}{2}b\right)^2 + \frac{3}{4}b^2$$

Theorème 3.4.5. *$\mathbb{Z}[j]$ est euclidien pour la norme.*

Démonstration. analogue à celle de $\mathbb{Z}[i]$. □

Application 3.4.1. Application de l'arithmétique de $\mathbb{Z}[i]$: résolution de l'équation :

$$x^2 + y^2 = N$$

Exemple 3.4.1. Résoudre $x^2 + y^2 = 13$, $x, y \in \mathbb{Z}$. On passe dans $\mathbb{Z}[i]$:

$$(x + iy)(x - iy) = 13$$

dans $\mathbb{Z}[i]$

$$13 = 2^2 + 3^2 = (2 + 3i)(2 - 3i)$$

$$(x + yi)(x - yi) = (2 + 3i)(2 - 3i)$$

On a :

$$N(2 + 3i) = 13 \qquad \text{nombre premier}$$

donc $2 + 3i$ est irréductible dans $\mathbb{Z}[i]$ et $N(2 - 3i) = 13$ donc $2 - 3i$ irréductible dans $\mathbb{Z}[i]$. Or $\mathbb{Z}[i]$ est euclidien pour la norme : le théorème fondamental de l'arithmétique est vérifié (décomposition en facteurs irréductibles). Donc : $\exists u \in U(\mathbb{Z}[i])$ tel que $x = yi = u(2 + 3i)$ ou $\exists v \in U(\mathbb{Z}[i])$ tel que : $x + yi = v(2 - 3i)$.

$$\begin{array}{lll} u = a + bi \in U(\mathbb{Z}[i]) & \Leftrightarrow & N(u) = a^2 + b^2 \\ \Leftrightarrow a = \pm 1 \text{ et } b = 0 \text{ ou } a = 0 \text{ et } b = \pm i & & \\ & \Leftrightarrow & u \in \{-1, 1, i, -i\} \end{array}$$

donc $x+yi = \pm(2+3i)$ ou $x+yi = \pm i(2+3i)$. Les solutions sont donc : $(2, 3)$, $(-2, -3)$ $(-2, 3)$, $(2, -3)$.